ESET SMART SECURITY 7

Benutzerhandbuch

(für Produktversion 7.0 und höher)

Microsoft® Windows® 8.1 / 8 / 7 / Vista / XP / Home Server 2003 / Home Server 2011

Klicken Sie hier, um die neueste Version dieses Dokuments herunterzuladen.



ESET SMART SECURITY

Weltweiter Support: www.eset.de/support

Versionsstand 5/13/2014

Inhalt

1. ESET Smart Security

ESET Smart Security ist ein neuer Ansatz für vollständig integrierte Computersicherheit. Die neueste Version des ThreatSense®-Prüfmoduls arbeitet in Kombination mit der perfekt abgestimmten Personal Firewall und dem Spam-Schutz schnell und präzise zum Schutz Ihres Computers. Auf diese Weise ist ein intelligentes System entstanden, das permanent vor Angriffen und bösartiger Software schützt, die Ihren Computer gefährden können.

ESET Smart Security ist eine umfassende Sicherheitslösung, die maximalen Schutz mit minimalen Anforderungen an die Systemressourcen verbindet. Die modernen Technologien setzen künstliche Intelligenz ein, um ein Eindringen von Viren, Spyware, Trojanern, Würmern, Adware, Rootkits und anderen Bedrohungen zu vermeiden, ohne dabei die Systemleistung zu beeinträchtigen oder die Computerprozesse zu unterbrechen.

Funktionen und Vorteile

Viren- und Spyware-Schutz	Erkennt und entfernt proaktiv eine größere Anzahl von bekannten und unbekannten Viren, Würmern, Trojanern und Rootkits. **Die Advanced Heuristik**-Technologie markiert selbst vollkommen neue Malware und schützt Ihren Computer vor unbekannten Bedrohungen, die abgewendet werden, bevor sie Schaden anrichten können. **Der Web-** und **Phishing-Schutz** überwacht die Kommunikation zwischen Webbrowsern und Remoteservern (einschließlich SSL-Verbindungen). **Der E-Mail-Client-Schutz** dient der Überwachung eingehender E-Mails, die mit dem POP3(S)- oder dem IMAP(S)-Protokoll übertragen werden.
Reguläre Updates	Das regelmäßige Aktualisieren der Signaturdatenbank und der Programmmodule gewährleistet einen optimalen Schutz Ihres Computers.
ESET Live Grid (Cloud-basierter Reputations-Check)	Sie können die Reputation ausgeführter Prozesse und Dateien direkt mit ESET Smart Security überprüfen.
Medienkontrolle	Prüft automatisch alle USB-Speicher, Speicherkarten und CDs/DVDs. Sperrt den Zugriff auf Wechselmedien anhand von Kriterien wie Medientyp, Hersteller, Größe und weiteren Attributen.
HIPS-Funktion	Sie können das Verhalten des Systems detailliert anpassen, Regeln für die Systemregistrierung und für aktive Prozesse und Programme festlegen und Ihre Sicherheitsposition genau konfigurieren.
Gamer-Modus	Unterdrückt Popup-Fenster, Updates und andere systemintensive Aktivitäten, um Systemressourcen für Spiele oder andere Anwendungen im Vollbildmodus zu bewahren.

Funktionen von ESET Smart Security

Kindersicherung	Schützt Ihre Familienmitglieder vor potenziell unerlaubten Webinhalten, indem bestimmte Websitekategorien blockiert werden.
Intelligente Firewall	Das Firewall-Modul verhindert, dass nicht autorisierte Benutzer auf Ihren Computer und Ihre persönlichen Daten zugreifen.
ESET-Spam-Schutz	Spam macht bis zu 80 Prozent der gesamten E-Mail-Kommunikation aus. Der Spam-Schutz nimmt dieses Problem in Angriff.
ESET Anti-Theft	ESET Anti-Theft bietet im Falle eines Verlusts oder Diebstahls des Computers eine erhöhte Sicherheit auf Benutzerebene. Nachdem der Benutzer ESET Smart Security installiert und ESET Anti-Theft aktiviert hat, wird das Gerät des Benutzers in der Weboberfläche aufgeführt. Über die Weboberfläche kann der Benutzer die Konfiguration von ESET Anti-Theft verwalten und Aktionen ausführen, z. B. einen Computer als verloren melden.

Die Funktionen von ESET Smart Security arbeiten nur mit einer ordnungsgemäß aktivierten Lizenz. Wir empfehlen,

die Lizenz für ESET Smart Security einige Wochen vor dem Ablauf zu verlängern.

1.1 Neuerungen in Version 7

ESET Smart Security Version 7 enthält zahlreiche kleine Verbeserungen:

- **Medienkontrolle** - Ersetzt die Funktion Wechselmedien aus den Versionen 5 und 6. Mit diesem Modul können Sie Medien bzw. Geräte prüfen oder sperren oder erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie ein Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten kann.
- **Schwachstellen-Schutz** - Eine Erweiterung der Personal Firewall, die die Erkennung bekannter Sicherheitslücken auf Netzwerkebene verbessert.
- **Exploit-Blocker** - Diese Komponente sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab.
- **Erweiterte Speicherprüfung** - Bietet im Zusammenspiel mit dem Exploit-Blocker stärkeren Schutz vor Schadsoftware, die Verschleierung und/oder Verschlüsselung einsetzt, um der Erkennung durch Anti-Malware-Produkte zu entgehen.
- **Firewall-Verbesserungen** - In der neuen Version von ESET Smart Security können Sie IDS-Ausnahmen und die vorübergehende Negativliste für IP-Adressen anpassen und verwalten. Die Benachrichtigungen über IDS-Erkennungen sind nun benutzerfreundlicher und informativer.
- **Verbesserungen des Phishing-Schutzes** – ESET Smart Security blockiert nun betrügerische wie auch Phishing-Seiten. Verbesserte Übermittlung von verdächtigen Seiten und Fehlalarmen durch die Anwender.
- **Spezielle Säuberungen** - Paket mit den 3-5 häufigsten kritischen Schadsoftware-Paketen.
- **Schnellere und zuverlässigere Installation** - Inklusive automatischer Anfangsprüfung 20 Minuten nach Installation und Neustart.
- **Kompatibilität des E-Mail-Plugins** - Unser Plugin kann nun in Office 2013 und Windows Live Mail integriert werden.
- **Verbesserte Kompatibilität unter Windows 8/8.1** - ESET SysRescue bietet nun auch unter Windows 8 den vollen Funktionsumfang. Dies gilt auch für Popup-Benachrichtigungen in Windows 8, die HIPS-Treffer oder erkannte Dateien melden, die einen Benutzereingriff erfordern, oder den Anwender über Downloads von potenziell unerwünschten Anwendungen informieren.

Weitere Details zu den neuen Funktionen in ESET Smart Security finden Sie im folgenden ESET Knowledgebase-Artikel:
Neuheiten in ESET Smart Security 7 und ESET NOD32 Antivirus 7?

1.2 Systemanforderungen

Für einen reibungslosen Betrieb von ESET Smart Security muss Ihr System die folgenden Hardware- und Softwareanforderungen erfüllen:

Microsoft® Windows® XP

600-MHz-Prozessor, 32 Bit (x86)/64 Bit (x64)
128 MB RAM
320 MB freier Speicherplatz auf der Festplatte
Super VGA (800 x 600)

Microsoft® Windows® 8.1, 8, 7, Vista

1-GHz-Prozessor, 32 Bit (x86)/64 Bit (x64)
512 MB RAM
320 MB freier Speicherplatz auf der Festplatte
Super VGA (800 x 600)

1.3 Prävention

Bei der Arbeit am Computer und besonders beim Surfen im Internet sollten Sie sich darüber im Klaren sein, dass kein Virenschutz der Welt die mit Infiltrationen und Angriffen einhergehenden Risiken gänzlich ausschließen kann.. Für maximalen Schutz und einen möglichst geringen Aufwand müssen Sie die Virenschutzsoftware richtig einsetzen und dabei einige wichtige Regeln beachten:

Führen Sie regelmäßige Updates durch

Gemäß von ESET Live Grid erhobenen Statistiken werden täglich tausende neuartige Schadprogramme zur Umgehung bestehender Sicherheitsmaßnahmen entwickelt, die den Entwicklern Vorteile auf Kosten anderer Benutzer verschaffen sollen. Die Experten aus dem Virenlabor von ESET analysieren diese Bedrohungen täglich und veröffentlichen Updates zur kontinuierlichen Verbesserung des Virenschutzes. Die richtige Konfiguration der Updates ist von wesentlicher Bedeutung für die Gewährleistung eines optimalen Schutzes. Weitere Informationen zur Konfiguration von Updates finden Sie im Kapitel Einstellungen für Updates.

Laden Sie Sicherheitspatches herunter

Die Entwickler von Schadsoftware nutzen oft Sicherheitslücken im System aus, um möglichst effektiv Schadcode zu verbreiten. Softwareunternehmen halten daher regelmäßig Ausschau nach neuen Sicherheitslücken in den eigenen Anwendungen und veröffentlichen Sicherheitsupdates zur Bekämpfung potenzieller Bedrohungen. Es ist wichtig, dass Sie diese Updates umgehend nach der Veröffentlichung herunterladen. Microsoft Windows und Webbrowser wie Internet Explorer sind Beispiele für Programme, für die regelmäßig Sicherheitsaktualisierungen veröffentlicht werden.

Sichern wichtiger Daten

Malware-Entwickler missachten die Interessen der Benutzer und legen mit ihrer Software oft das gesamte Betriebssystem lahm bzw. nehmen den Verlust wichtiger Daten bewusst in Kauf. Es ist wichtig, dass Sie Ihre wichtigen und vertraulichen Daten regelmäßig auf einem externen Speichermedium (z. B. einer DVD oder einer externen Festplatte) sichern. So können Sie Ihre Daten bei einem Systemfehler viel einfacher und schneller wiederherstellen.

Prüfen Sie Ihren Computer regelmäßig auf Viren

Der Echtzeit-Dateischutz erkennt eine größere Zahl bekannter und unbekannter Viren, Würmer, Trojaner und Rootkits. Jedes Mal, wenn Sie eine Datei öffnen oder auf eine Datei zugreifen, wird die Datei auf Schadcode überprüft. Wir empfehlen jedoch, dass Sie mindestens einmal im Monat eine vollständige Prüfung des Computers ausführen, da Schadcode die verschiedensten Formen annehmen kann und die Signaturdatenbank täglich aktualisiert wird.

Halten Sie grundlegende Sicherheitsregeln ein

Die nützlichste und effektivste Regel von allen ist das Prinzip ständiger Wachsamkeit. Heutzutage erfordert ein Großteil der Schadsoftware zur Ausführung und Ausbreitung ein Eingreifen des Benutzers. Wenn Sie beim Öffnen neuer Dateien achtsam sind, sparen Sie viel Zeit und Aufwand, die Sie andernfalls darauf verwenden müssten, eingedrungene Schadsoftware zu entfernen. Hier finden Sie einige nützliche Richtlinien:

- Besuchen Sie keine zweifelhaften Websites, die durch zahlreiche Popup-Fenster und bunte Werbeanzeigen auffallen.
- Seien Sie vorsichtig bei der Installation von Programmen, Codec-Paketen usw. Verwenden Sie nur sichere Programme, und besuchen Sie ausschließlich sichere Websites.
- Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen, insbesondere wenn es sich um Anhänge von Massen-E-Mails und E-Mail-Nachrichten mit unbekanntem Absender handelt.
- Verwenden Sie für die tägliche Arbeit mit dem Computer kein Administratorkonto.

2. Installation

Zur Installation von ESET Smart Security auf Ihrem Computer stehen verschiedene Methoden zur Verfügung. Die verfügbaren Installationsmethoden unterscheiden sich je nach Land und Vertriebsart:

- Der Live-Installer kann von der ESET-Website heruntergeladen werden. Das Installationspaket gilt für alle Sprachen (wählen Sie die gewünschte Sprache aus). Live-Installer ist eine kleine Datei. Zusätzlich für die Installation von ESET Smart Security erforderliche Dateien werden automatisch heruntergeladen.

- Offline-Installation - Diese Art der Installation wird beim Installieren von einer CD/DVD verwendet. Die hierbei verwendete *.msi*-Datei ist größer als die Live-Installer-Datei. Zur Installation sind jedoch keine zusätzlichen Dateien und keine Internetverbindung erforderlich.

Wichtig: Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind, bevor Sie mit der Installation von ESET Smart Security beginnen. Anderenfalls kann es zu Konflikten zwischen den Programmen kommen. Wir empfehlen Ihnen, alle anderen Virusschutzprogramme zu deinstallieren. Eine Liste von Tools zum Deinstallieren üblicher Virenschutzsoftware finden Sie in unserem ESET-Knowledgebase-Artikel (in englischer und in bestimmten weiteren Sprachen verfügbar).

2.1 Live-Installer

Nachdem Sie das *Live-Installer*-Installationspaket heruntergeladen haben, doppelklicken Sie auf die Installationsdatei und befolgen Sie die schrittweisen Anweisungen im Installationsfenster.

Wichtig: Für diese Art der Installation ist eine Internetverbindung erforderlich.



Wählen Sie im Dropdown-Menü **Produktsprache wählen** die gewünschte Sprache aus und klicken Sie auf **Installieren**. Warten Sie einen Moment, bis die Installationsdateien heruntergeladen wurden.

Nach dem Sie die **Endbenutzer-Softwarelizenzvereinbarung** akzeptiert haben, werden Sie zur Konfiguration von **ESET Live Grid** aufgefordert. ESET Live Grid stellt sicher, dass ESET sofort und fortlaufend über neue Bedrohungen informiert wird, um unsere Kunden zu schützen. Das System übermittelt neue Bedrohungen an das ESET-Virenlabor, wo die entsprechenden Dateien analysiert, bearbeitet und zur Signaturdatenbank hinzugefügt werden.

Standardmäßig ist die Option **Ja, ich möchte teilnehmen** ausgewählt und die Funktion somit aktiviert.

Im nächsten Schritt der Installation wird die Prüfung auf eventuell unerwünschte Anwendungen konfiguriert. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können. Weitere Details finden Sie im Kapitel Eventuell unerwünschte Anwendungen.

Klicken Sie auf **Weiter**, um die Installation zu beginnen.

2.2 Offline-Installation

Nachdem Sie das Offline-Installationspaket (.msi) gestartet haben, führt der Installationsassistent Sie durch die Einstellungen.



Das Programm überprüft zunächst, ob eine neuere Version von ESET Smart Security verfügbar ist. Wenn eine neuere Version erkannt wird, werden Sie im ersten Schritt der Installation darauf hingewiesen. Wenn Sie nun die Option **Neue Version herunterladen und installieren** wählen, wird die neue Version heruntergeladen und die Installation fortgesetzt. Dieses Kontrollkästchen ist nur sichtbar, wenn eine neuere Version als diejenige, die Sie gerade installieren, verfügbar ist.

Im nächsten Schritt wird die Endbenutzer-Lizenzvereinbarung angezeigt. Lesen Sie sich diese Vereinbarung sorgfältig durch. Wenn Sie damit einverstanden sind, klicken Sie auf **Ich stimme zu**. Nachdem Sie die Vereinbarung angenommen haben, wird die Installation fortgesetzt.

Weitere Anweisungen zu den Installationsschritten, zu **ESET Live Grid** und zu **Prüfen auf evtl. unerwünschte Anwendungen** finden Sie im Abschnitt zum Live-Installer.



Bei der Installation wird eine Konfiguration verwendet, die für die Anforderungen der meisten Benutzer geeignet ist. Die vorgegebenen Einstellungen bieten sehr gute Sicherheit in Verbindung mit einfacher Konfiguration und hoher Systemleistung. **Die erweiterten Einstellungen** sind für erfahrene Benutzer geeignet, die während der Installation spezielle Einstellungen vornehmen möchten. Klicken Sie auf **Installieren**, um den Installationsprozess zu starten und die erweiterten Einstellungen zu umgehen.

2.2.1 Erweiterte Einstellungen

Nach der Auswahl von **Erweiterte Einstellungen** werden Sie dazu aufgefordert, einen Speicherort für die Installation auszuwählen. Standardmäßig wird das Programm in folgendes Verzeichnis installiert:

C:\Programme\ESET\ESET Smart Security

Klicken Sie auf **Durchsuchen**, um diesen Speicherort zu ändern (nicht empfohlen).

Klicken Sie auf **Weiter**, um die Einstellungen für Internetverbindung festzulegen. Wenn Sie einen Proxyserver verwenden, muss dieser richtig eingestellt sein, damit die Signaturdatenbank aktualisiert werden kann. Wenn Sie sich nicht sicher sind, ob Sie zur Verbindung mit dem Internet einen Proxyserver verwenden, wählen Sie **Einstellungen aus Internet Explorer übernehmen (empfohlen)** und klicken Sie auf **Weiter**. Wenn Sie keinen Proxyserver verwenden, wählen Sie die Option **Keinen Proxyserver verwenden**.

Um die Einstellungen für Ihren Proxyserver zu konfigurieren, wählen Sie **Ich nutze einen Proxyserver** und klicken Sie auf **Weiter**. Geben Sie unter **Adresse** die IP-Adresse oder URL des Proxyservers ein. Im Feld **Port** können Sie den Port angeben, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Falls für den Proxyserver Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie einen gültigen **Benutzernamen** und das **Passwort** ein. Die Einstellungen für den Proxyserver können auch aus dem Internet Explorer kopiert werden, falls gewünscht. Klicken Sie dazu auf **Übernehmen**, und bestätigen Sie die Auswahl.

Wenn Sie „Benutzerdefinierte Installation“ wählen, können Sie festlegen, wie Ihr System mit automatischen Programm-Updates verfahren soll. Klicken Sie auf **Ändern...**, um zu den erweiterten Einstellungen zu gelangen.

Wenn Sie nicht möchten, dass Programmkomponenten aktualisiert werden, wählen Sie **Niemals ausführen**. Wenn Sie die Option **Benutzer fragen** auswählen, wird vor dem Herunterladen von Programmkomponenten ein Bestätigungsfenster angezeigt. Um Programmkomponenten automatisch zu aktualisieren, wählen Sie **Immer ausführen**.

HINWEIS: Nach der Aktualisierung von Programmkomponenten muss der Computer üblicherweise neu gestartet werden. Wir empfehlen die Einstellung **Computer bei Bedarf ohne Benachrichtigung neu starten**.

Im nächsten Installationsfenster haben Sie die Möglichkeit, die Einstellungen des Programms mit einem Passwort zu schützen. Wählen Sie die Option **Einstellungen mit Passwort schützen** und geben Sie ein Passwort in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein. Dieses Passwort ist anschließend erforderlich, um die Einstellungen von ESET Smart Security zu ändern bzw. auf die Einstellungen zuzugreifen. Wenn beide Passwortfelder übereinstimmen, fahren Sie mit **Weiter** fort.

Befolgen Sie zum Abschließen der weiteren Installationsschritte (**ESET Live Grid** und **Prüfen auf „Evtl. unerwünschte Anwendungen“**) die Anweisungen im Abschnitt zum Live-Installer.

Wählen Sie als Nächstes den Filtermodus für die Personal Firewall von ESET. Für die ESET Smart Security Personal Firewall stehen vier Filtermodi zur Verfügung. Das Verhalten der Firewall ist davon abhängig, welcher Modus ausgewählt wurde. Die Filtermodi bestimmen gleichzeitig, in welchem Umfang Benutzereingriffe erforderlich sind.

Um die Erstprüfung nach der Installation zu deaktivieren, die Ihren Compuer normalerweise nach Abschluss der Installation auf Schadsoftware prüft, deaktivieren Sie das Kontrollkästchen neben **Nach Installation prüfen**. Klicken Sie im Fenster **Bereit zur Installation** auf **Installieren**, um die Installation abzuschließen.

2.3 Produktaktivierung

Nach Abschluss der Installation werden Sie aufgefordert, Ihr Produkt zu aktivieren.

Zur Aktivierung des Produkts stehen verschiedene Methoden zur Verfügung. Die Verfügbarkeit einer bestimmten Aktivierungsmöglichkeit im Aktivierungsfenster hängt vom Land und von der Vertriebsart (CD/DVD, ESET-Webseite usw.) ab.

Wenn Sie das Produkt in einer Einzelhandelsverpackung erworben haben, wählen Sie **Aktivierung mithilfe eines Aktivierungscodes** aus. Den Aktivierungscode finden Sie normalerweise in der Produktverpackung oder auf deren Rückseite. Der Aktivierungscode muss unverändert eingegeben werden, damit die Aktivierung erfolgreich ausgeführt werden kann.

Wenn Sie einen Benutzernamen und ein Passwort erhalten haben, wählen Sie **Aktivierung mithilfe eines Benutzernamens und eines Passworts** und geben Sie die Daten in die entsprechenden Felder ein.

Wenn Sie ESET Smart Security vor dem Kauf testen möchten, wählen Sie **Testlizenz aktivieren**. Geben Sie Ihre E-Mail-Adresse und Ihr Land ein, um ESET Smart Security für einen begrenzten Zeitraum zu aktivieren. Sie erhalten die Testlizenz per E-Mail. Eine Testlizenz kann pro Kunde nur ein einziges Mal aktiviert werden.

Wenn Sie noch keine Lizenz haben und eine erwerben möchten, klicken Sie auf **Lizenz kaufen**. Hiermit gelangen Sie zur Website Ihres lokalen ESET-Distributors.

Wählen Sie **Später aktivieren**, wenn Sie das Produkt zunächst als Testversion beurteilen und nicht sofort aktivieren möchten, oder wenn Sie das Produkt zu einem späteren Zeitpunkt aktivieren möchten.

Sie können Ihre Installation von ESET Smart Security auch direkt aus dem Programm aktivieren. Klicken Sie in der oberen rechten Ecke auf das Symbol Programmmenü oder klicken Sie mit der rechten Maustaste auf das ESET Smart Security-Symbol in der Taskleiste und wählen Sie **Produktaktivierung** aus dem Menü aus.

2.4 Benutzername und Passwort eingeben

Damit alle Funktionen optimal genutzt werden können, sollte das Programm automatisch aktualisiert werden. Dies ist nur möglich, wenn die korrekten Lizenzdaten (Benutzername und Passwort) unter **Einstellungen für Updates** eingegeben wurden.

Falls Sie Ihren Benutzernamen und das Passwort während des Installationsvorgangs nicht eingegeben haben, können Sie dies nun vornehmen. Klicken Sie im Hauptprogrammfenster auf **Hilfe und Support** und dann auf **Produktaktivierung**. Geben Sie im Fenster zur Produktaktivierung die Lizenzdaten ein, die Sie für Ihr ESET Security-Produkt erhalten haben.

Bei der Eingabe von **Benutzername** und **Passwort** muss deren Formatierung exakt beachtet werden:

- Bei Benutzername und Passwort muss die Groß- und Kleinschreibung beachtet. Achten Sie auf den Bindestrich im Benutzernamen.
- Das Passwort besteht aus 10 Zeichen in Kleinschreibung.
- Der Buchstabe L wird im Passwort nicht verwendet (verwenden Sie stattdessen die Zahl 1).
- Das große Zeichen „0“ ist die Nummer null (0); das kleine „o“ ist der kleingeschriebene Buchstabe o.

Wir empfehlen, die Daten durch Kopieren und Einfügen aus der Registrierungs-E-Mail zu übernehmen, um Tippfehler zu vermeiden.

2.5 Upgrade auf eine aktuellere Version

Neuere Versionen von ESET Smart Security werden veröffentlicht, um Verbesserungen oder Patches durchzuführen, die ein automatisches Update der Programmmodule nicht leisten kann. Es gibt verschiedene Möglichkeiten, ein Upgrade auf eine aktuellere Version durchzuführen:

1. Automatische Aktualisierung durch ein Programm-Update
   Da das Programm-Update an alle Benutzer des Programms ausgegeben wird und Auswirkungen auf bestimmte Systemkonfigurationen haben kann, wird es erst nach einer langen Testphase veröffentlicht, wenn sicher ist, dass es in allen möglichen Konfigurationen funktioniert. Wenn Sie sofort nach der Veröffentlichung eines Upgrades auf die neue Version aufrüsten möchten, befolgen Sie eine der nachstehenden Methoden.

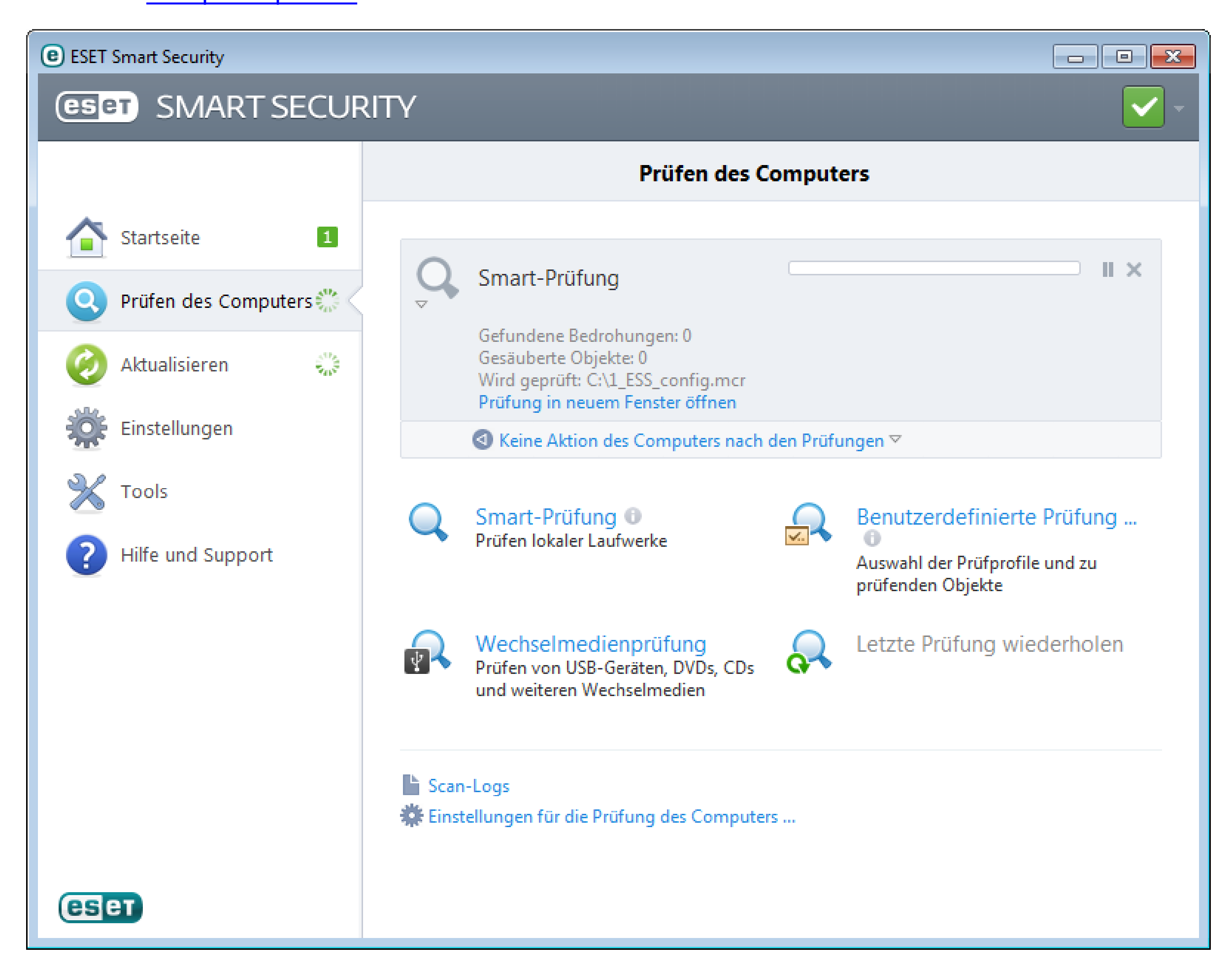
2. Manuelle Aktualisierung, indem Sie im Bereich **Update** auf **Installieren/Nach Updates suchen** klicken

3. Manuelle Aktualisierung durch Herunterladen und Installieren der aktuelleren Version (ohne Deinstallation der vorherigen Version)

2.6 Erstprüfung nach Installation

Nach der Installation von ESET Smart Security wird der Computer 20 Minuten nach der Installation oder nach einem Neustart auf Schadsoftware geprüft.

Sie können die Prüfung des Computers auch manuell aus dem Haupt-Programmfenster auslösen, indem Sie auf **Computer prüfen** > **Smart-Prüfung** klicken. Weitere Informationen zur Prüfung des Computers finden Sie im Abschnitt Computer prüfen.



3. Erste Schritte

Dieses Kapitel enthält eine einführende Übersicht über ESET Smart Security und die Grundeinstellungen des Programms.

3.1 Das Haupt-Programmfenster

Das Hauptprogrammfenster von ESET Smart Security ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

Im Folgenden werden die Optionen des Hauptmenüs beschrieben:

Startseite - Informationen zum Schutzstatus von ESET Smart Security.

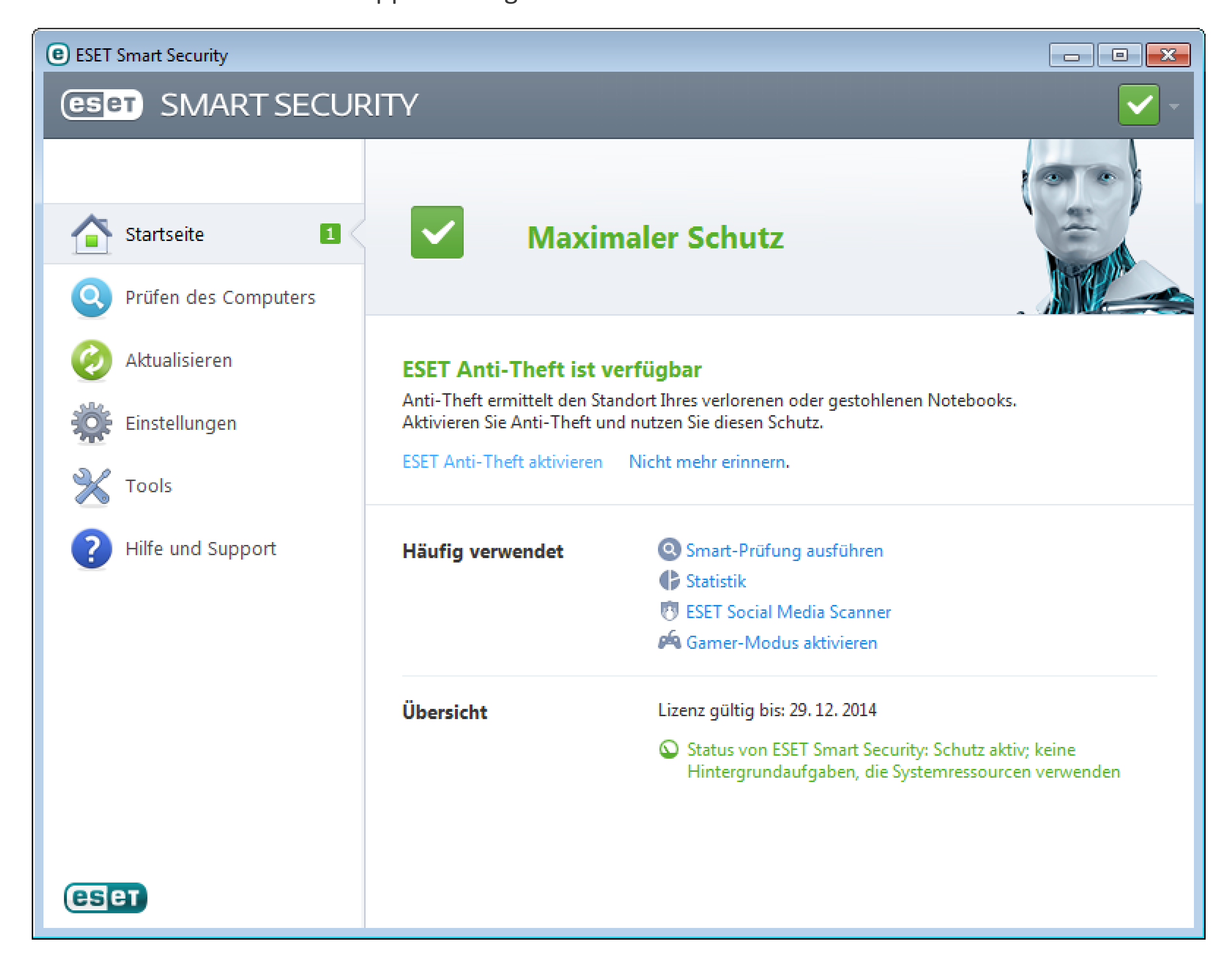
Computer prüfen - In diesem Abschnitt können Sie eine Smart-Prüfung oder eine Prüfung mit speziellen Einstellungen starten.

Update - Dieser Bereich zeigt Informationen zu Updates der Signaturdatenbank an.

Einstellungen - Mit dieser Option können Sie das Maß an Sicherheit für Ihren Computer, Ihre Internetverbindung und Ihre E-Mailssowie Ihr Netzwerk und die Kindersicherung anpassen..

Tools - Zugang zu den Log-Dateien, der Anzeige der Schutzstatistik, den Funktionen „Aktivität beobachten“ und „Ausgeführte Prozesse“,Netzwerkverbindungen,Taskplaner, Quarantäne sowie zu ESET SysInspector und ESET SysRescue.

Hilfe und Support - Dieser Bereich bietet Zugriff auf die Hilfedateien, die ESET-Knowledgebase, die Website von ESET und das Formular für Supportanfragen.



Die **Startseite** enthält Informationen über die Sicherheit und die aktuelle Schutzstufe Ihres Computers. Im Statusfenster werden auch die am häufigsten verwendeten Funktionen von ESET Smart Security angezeigt. Unter **Übersicht** finden Sie auch das Ablaufdatum Ihrer Lizenz.

 Das grüne Schutzstatussymbol zeigt an, dass **Maximaler Schutz** gewährleistet ist.

Vorgehensweise bei fehlerhafter Ausführung des Programms

Wenn die aktivierten Module ordnungsgemäß arbeiten, wird ein grünes Schutzstatussymbol angezeigt. Ein rotes Ausrufezeichen oder ein oranger Hinweis weisen auf ein nicht optimales Schutzniveau hin. Unter **Startseite** werden zusätzliche Informationen zum Schutzstatus der einzelnen Module und empfohlene Lösungen zum Wiederherstellen des vollständigen Schutzes angezeigt. Um den Status einzelner Module zu ändern, klicken Sie auf **Einstellungen** und wählen Sie das gewünschte Modul aus.



 Das rote Symbol und der Status „Maximaler Schutz ist nicht gewährleistet“ weisen auf kritische Probleme hin. Dieser Status kann verschiedene Ursachen haben, zum Beispiel:

- **Produkt nicht aktiviert** - Sie können ESET Smart Security entweder auf der **Startseite** unter **Vollversion aktivieren** oder unter Schutzstatus über die Schaltfläche **Jetzt kaufen** aktivieren.
- **Signaturdatenbank nicht mehr aktuell** - Dieser Fehler wird angezeigt, wenn die Signaturdatenbank trotz wiederholter Versuche nicht aktualisiert werden konnte. Sie sollten in diesem Fall die Update-Einstellungen überprüfen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten oder fehlerhaft konfigurierte Verbindungseinstellungen.
- **Viren- und Spyware-Schutz deaktiviert** - Sie können den Virenschutz und den Spyware-Schutz wieder aktivieren, indem Sie auf **Alle Module des Viren- und Spyware-Schutzes aktivieren** klicken.
- **ESET Personal Firewall deaktiviert** - Dieser Zustand wird durch einen Sicherheitshinweis neben **Netzwerk** signalisiert. Sie können den Netzwerkschutz wieder aktivieren, indem Sie auf **Filtermodus aktivieren** klicken.
- **Lizenz ist abgelaufen** - Bei diesem Zustand ist das Schutzstatussymbol rot. Bei abgelaufener Lizenz kann das Programm keine Updates mehr durchführen. Wir empfehlen Ihnen, die in der Warnung angezeigten Anweisungen zur Verlängerung Ihrer Lizenz auszuführen.



Das orange Symbol bedeutet, dass Ihr Computer nur eingeschränkt geschützt ist. Möglicherweise bestehen Probleme bei der Aktualisierung des Programms, oder Ihre Lizenz läuft demnächst ab.
Dieser Status kann verschiedene Ursachen haben, zum Beispiel:

- **Anti-Theft-Optimierungswarnung** - Gerät ist nicht vollständig für ESET Anti-Theft optimiert. Ein Phantomkonto ist anfangs zum Beispiel nicht vorhanden. Es handelt sich hierbei um eine Sicherheitsfunktion, die automatisch ausgelöst wird, wenn Sie ein Gerät als vermisst kennzeichnen. Möglicherweise müssen Sie in der ESET Anti-Theft-Weboberfläche über die Funktion Optimierung ein Phantomkonto erstellen.

- **Gamer-Modus aktiviert** - Im Gamer-Modus besteht ein erhöhtes Risiko. Ist dieser Modus aktiviert, so werden alle Popup-Fenster deaktiviert und die Aktivität des Taskplaners wird komplett gestoppt.

- **Lizenz läuft bald ab** - Dieser Status wird durch ein Schutzstatussymbol mit einem Ausrufezeichen neben der Systemuhr angezeigt. Nach dem Ablaufen der Lizenz ist kein Programm-Update mehr möglich und das Schutzstatussymbol ist rot.

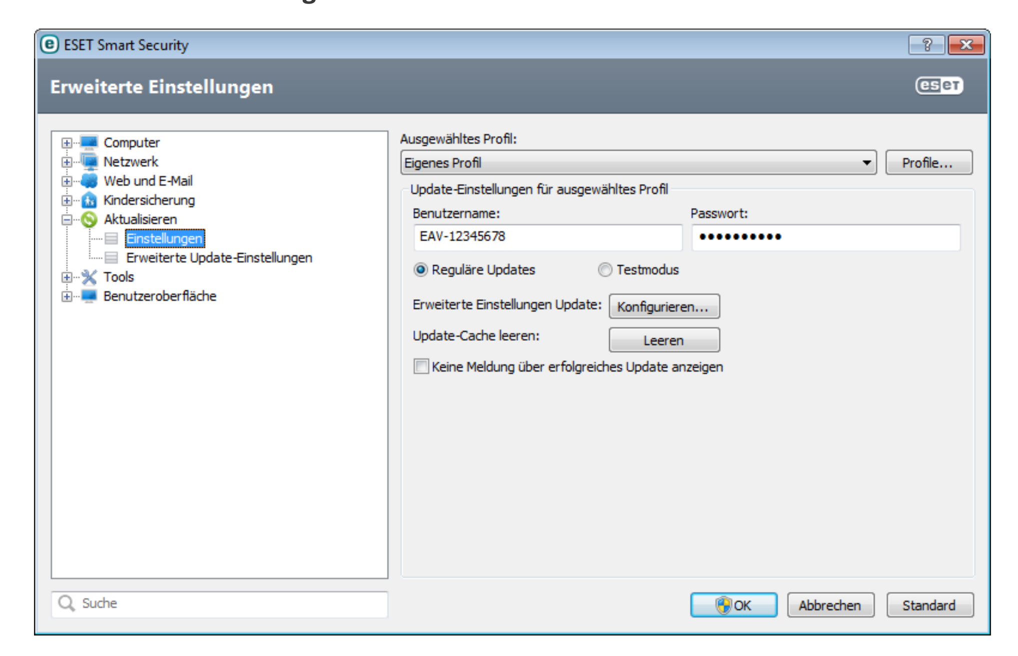
Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beseitigen können, klicken Sie auf **Hilfe und Support**, um zu den Hilfedateien oder der ESET-Knowledgebase zu gelangen. Wenn Sie weiterhin Unterstützung benötigen, können Sie eine Support-Anfrage senden. Unser Support wird sich umgehend mit Ihnen in Verbindung setzen, um Ihre Fragen zu beantworten und Lösungen für Ihr Problem zu finden.

3.2 Updates

Updates der Signaturdatenbank und Updates von Programmkomponenten sind eine wichtige Maßnahmen, um Ihr System vor Schadcode zu schützen. Achten Sie auf eine sorgfältige Konfiguration und Ausführung der Updates. Klicken Sie im Hauptmenü auf **Update** und dann auf **Signaturdatenbank aktualisieren**, um nach einem Update für die Signaturdatenbank zu suchen.

Wenn die Lizenzdaten (Benutzername und Passwort) während der Aktivierung von ESET Smart Security nicht eingegeben wurden, werden Sie nun dazu aufgefordert.

Das Fenster „Erweiterte Einstellungen“ (klicken Sie im Hauptmenü auf **Einstellungen** und dann auf **Erweiterte Einstellungen...** oder drücken Sie **F5** auf Ihrer Tastatur) enthält zusätzliche Update-Optionen. Klicken Sie links in der Baumstruktur der erweiterten Einstellungen auf **Update** > **Einstellungen**. Um erweiterte Update-Optionen wie den Update-Modus, den Proxyserverzugriff und die LAN-Verbindungen konfigurieren zu können, klicken Sie im **Update**-Fenster auf **Einstellungen...**.



3.3 Einstellungen vertrauenswürdige Zone

Die Einrichtung einer vertrauenswürdigen Zone ist notwendig, um Ihren Computer in einer Netzwerkumgebung zu schützen. Sie können anderen Benutzern Zugriff auf Ihren Computer gewähren, indem Sie die vertrauenswürdige Zone konfigurieren und Freigaben zulassen. Klicken Sie auf **Einstellungen** > **Netzwerk** > **Schutzmodus Ihres Computers im Netzwerk ändern**. In einem Fenster werden nun Optionen angezeigt, aus denen Sie den gewünschten Schutzmodus Ihres Computers im Netzwerk auswählen können.

Die Erkennung der vertrauenswürdigen Zone erfolgt entweder nach der Installation von ESET Smart Security oder nachdem der Computer mit einem neuen Netzwerk verbunden wurde. In den meisten Fällen muss die vertrauenswürdige Zone daher nicht definiert werden. Standardmäßig wird bei Erkennung einer neuen Zone ein Dialogfenster angezeigt, in dem Sie die Schutzstufe für diese Zone festlegen können.



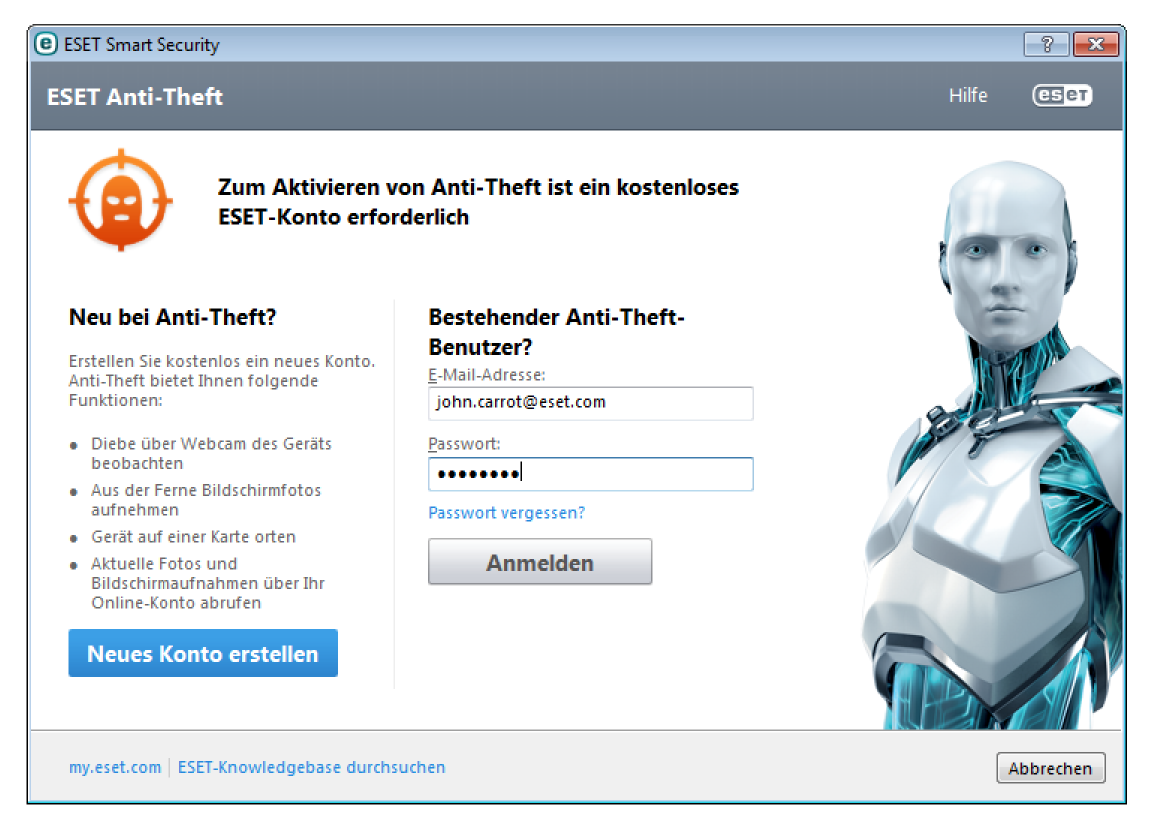
Warnung: Eine falsche Konfiguration der vertrauenswürdigen Zone kann ein Sicherheitsrisiko für Ihren Computer darstellen.

HINWEIS: Computer innerhalb der vertrauenswürdigen Zone erhalten standardmäßig Zugriff auf freigegebene Dateien und Drucker, die RPC-Kommunikation ist aktiviert, und Remotedesktopverbindungen sind möglich.

3.4 Anti-Theft

Um Ihren Computer im Falles eines Verlusts oder Diebstahls zu schützen, können Sie ihn über eine der folgenden Optionen beim ESET Anti-Theft-System registrieren.

1. Klicken Sie nach der erfolgreichen Aktivierung auf **Anti-Theft aktivieren**, um die Funktionen von ESET Anti-Theft für den soeben registrierten Computer zu aktivieren.



2. Wenn der Hinweis **ESET Anti-Theft ist verfügbar** auf der **Startseite** von ESET Smart Security angezeigt wird, sollten Sie abwägen, ob Sie diese Funktion für Ihren Computer aktivieren möchten. Klicken Sie auf **ESET Anti-Theft aktivieren**, um Ihren Computer mit ESET Anti-Theft zu verknüpfen.

3. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** und anschließend auf **ESET Anti-Theft**. Befolgen Sie die Anweisungen im Popup-Fenster.

Hinweis: ESET Anti-Theft ist nicht für den Einsatz auf Microsoft Windows Home Server geeignet.

Weitere Informationen über das Verknüpfen eines Computers mit ESET Anti-Theft finden Sie unter Hinzufügen eines neuen Geräts.

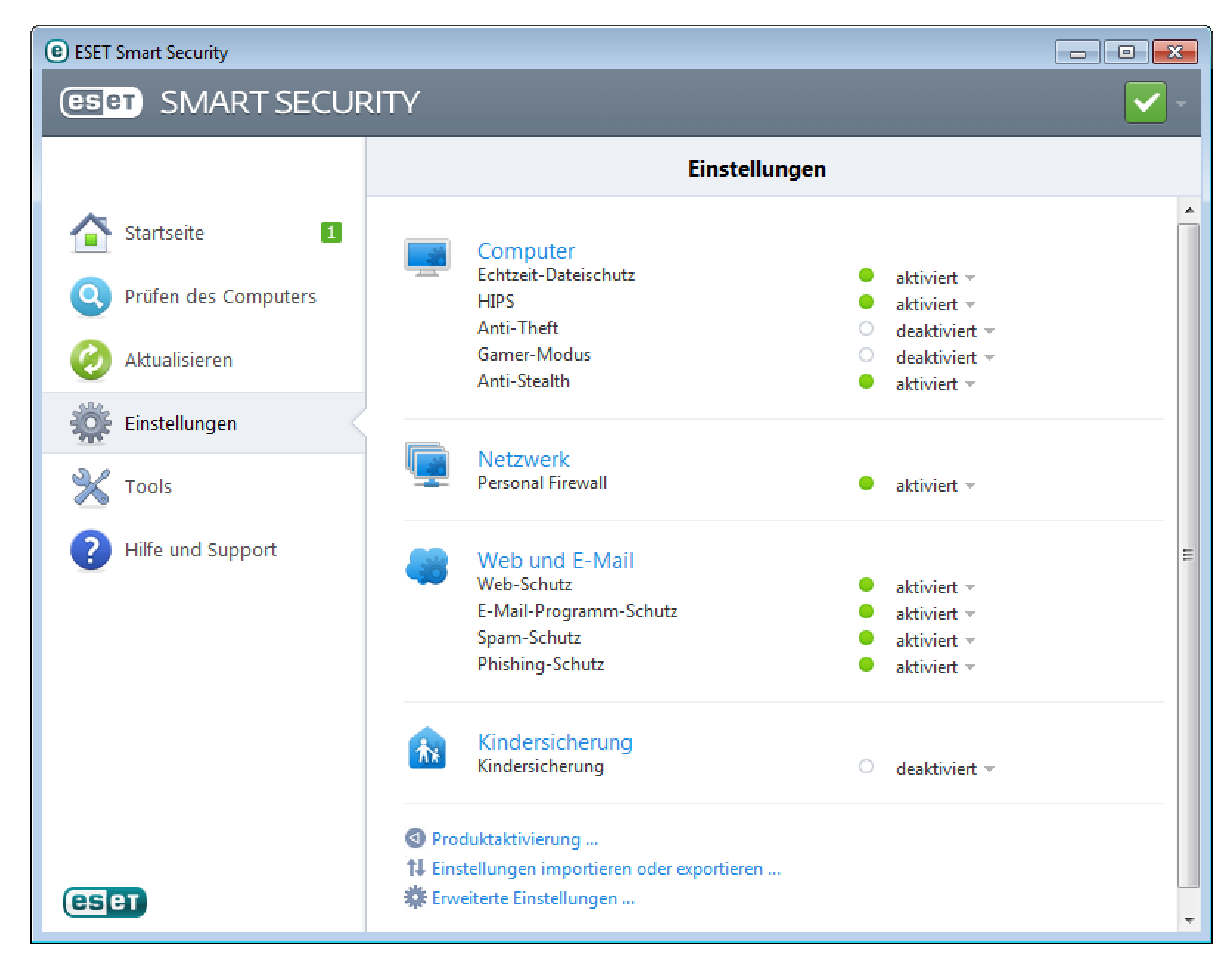
3.5 Kindersicherungs-Tools

Auch wenn Sie die Kindersicherung in ESET Smart Security bereits aktiviert haben, müssen Sie sie für die gewünschten Benutzerkonten konfigurieren, damit sie ordnungsgemäß funktioniert.

Wenn die Kindersicherung aktiviert, jedoch keine Benutzerkonten konfiguriert wurden, wird der Hinweis **Kindersicherung nicht eingerichtet** auf der **Startseite** des Hauptprogrammfensters angezeigt. Klicken Sie auf **Regeln jetzt einrichten** und erstellen Sie Regeln, um Ihre Kinder vor möglicherweise ungeeigneten Inhalten zu schützen. Anweisungen zum Erstellen von Regeln finden Sie im Kapitel Kindersicherung.

4. Arbeiten mit ESET Smart Security

Über das ESET Smart Security-Menü „Einstellungen“ können Sie die Schutzstufen für Ihren Computer und das Netzwerk anpassen.



Folgende Optionen stehen im Menü **Einstellungen** zur Verfügung:

- **Computer**
- **Netzwerk**
- **Web und E-Mail**
- **Kindersicherung**

Klicken Sie auf die gewünschte Komponente, um die erweiterten Einstellungen des entsprechenden Schutzmoduls anzupassen.

In den Einstellungen für den **Computer**-Schutz können Sie folgende Komponenten aktivieren oder deaktivieren:

- **Echtzeit-Dateischutz** - Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft.
- **HIPS** - Das HIPS-System überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß individueller Regeln aus.
- **Anti-Theft** - Hier können Sie ESET Anti-Theft auch aktivieren bzw. deaktivieren.
- **Gamer-Modus** - Aktiviert / deaktiviert den Gamer-Modus. Nach der Aktivierung des Gamer-Modus wird eine Warnung angezeigt (erhöhtes Sicherheitsrisiko) und das Hauptfenster wird orange.
- **Anti-Stealth** - Erkennt gefährliche Programme, wie Rootkits, die sich vor dem Betriebssystem und vor üblichen Erkennungsmethoden verbergen können.

Im Bereich **Netzwerk** können Sie die Personal Firewall aktivieren bzw. deaktivieren.

Mit der Kindersicherung können Sie Webseiten sperren, die potenziell Unerlaubtes enthalten könnten. Außerdem können Eltern mit dieser Funktion den Zugriff auf über 40 vordefinierte Webseitenkategorien und über 140

Unterkategorien unterbinden.

In den Einstellungen für Web und E-Mail-Schutz können Sie folgende Komponenten aktivieren oder deaktivieren:

- **Web-Schutz** - Wenn diese Option aktiviert ist, werden alle Daten geprüft, die über HTTP oder HTTPS übertragen werden.
- **E-Mail-Client-Schutz** - Überwacht eingehende E-Mails, die mit dem POP3- oder dem IMAP-Protokoll übertragen werden.
- **Spam-Schutz** - Prüft unerwünschte E-Mails (Spam).
- **Phishing-Schutz** – Filtert Websites, für die der Verdacht besteht, dass sie Inhalte enthalten, die den Benutzer zum Einreichen vertraulicher Informationen verleiten.

Zur Reaktivierung des Schutzes dieser Sicherheitskomponente klicken Sie auf **Deaktiviert** und anschließend auf **Aktivieren**.

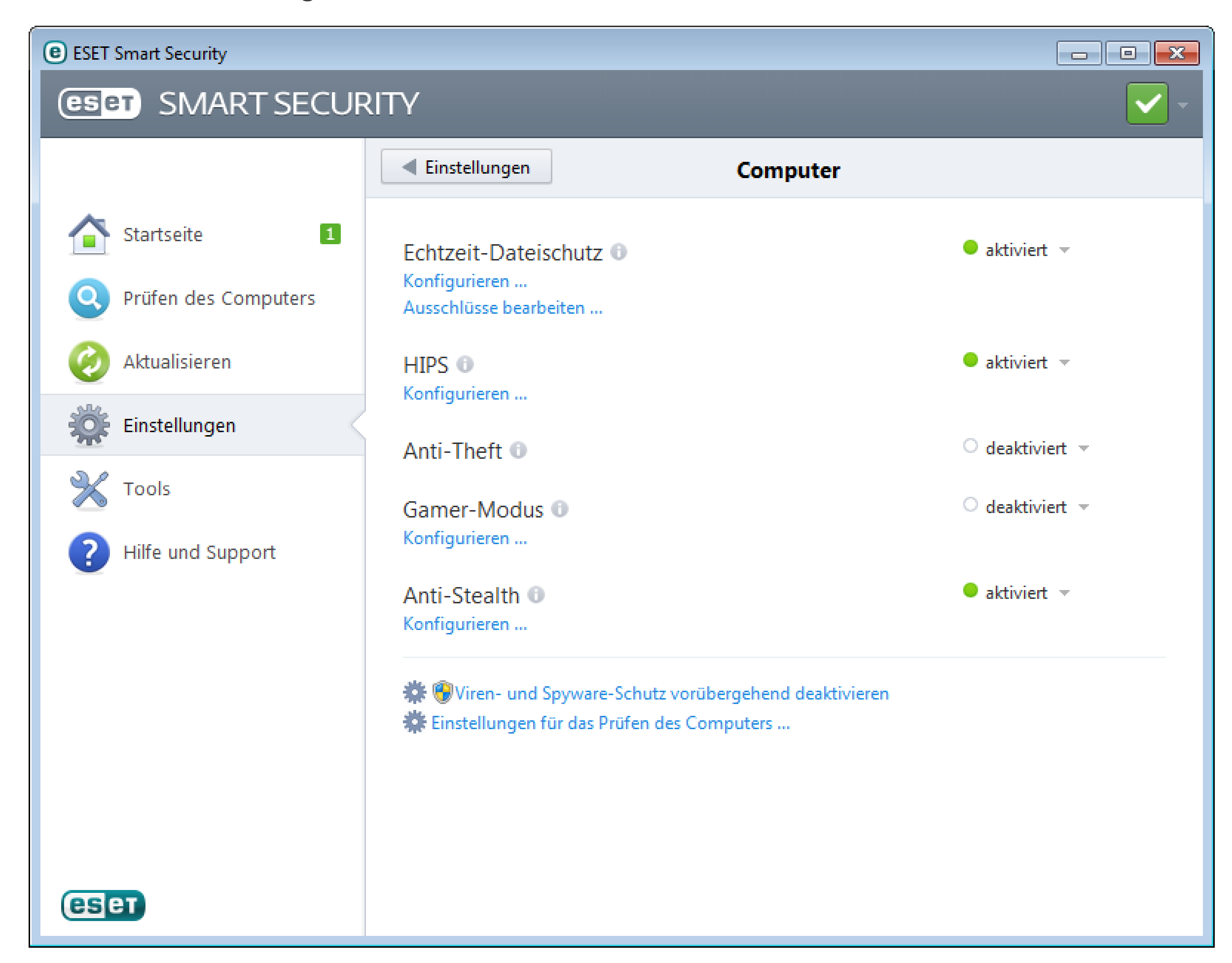
HINWEIS: Wenn Sie den Schutz auf diese Weise deaktivieren, werden alle deaktivierten Schutzkomponenten nach einem Computerneustart wieder aktiviert.

Am unteren Rand des Fensters „Einstellungen“ finden Sie weitere Optionen. Klicken Sie auf **Produktaktivierung**, um ein Registrierungsformular zu öffnen, mit dem Sie Ihr ESET Security-Produkt aktivieren können. Sie erhalten eine E-Mail mit den Lizenzdaten (Benutzername und Passwort). Verwenden Sie die Option **Einstellungen importieren/exportieren**, um die Einstellungen aus einer *XML*-Konfigurationsdatei zu laden oder die aktuellen Einstellungen in einer Konfigurationsdatei zu speichern.

4.1 Computer

Um den Abschnitt **Computer** zu öffnen, klicken Sie im Bereich **Einstellungen** auf **Computer**. Dieses Fenster gibt einen Überblick über alle Schutzmodule. Zur vorübergehenden Deaktivierung einzelner Module klicken Sie neben dem gewünschten Modul auf **Aktiviert** > **Deaktivieren für...**. Beachten Sie, dass dies den Schutz Ihres Computers beeinträchtigen kann. Um detaillierte Einstellungen für jedes Modul vorzunehmen, klicken Sie auf **Einstellungen**.

Klicken Sie auf **Ausschlussfilter bearbeiten**, um das Fenster Ausschlussfilter zu öffnen. Dort können Sie Dateien und Ordner von der Prüfung ausschließen.



Viren- und Spyware-Schutz vorübergehend deaktivieren - Deaktiviert alle Viren- und Spyware-Schutzmodule. Wenn Sie den Schutz deaktivieren, wird das Fenster **Schutz vorübergehend deaktivieren** angezeigt. Hier können Sie festlegen, wie lange der Schutz deaktiviert werden soll, indem Sie im Dropdown-Menü **Zeitraum** einen entsprechenden Wert auswählen. Klicken Sie zur Bestätigung auf **OK**.

Einstellungen für Prüfung... - Klicken Sie zur Anpassung der Parameter der On-Demand-Prüfung (manuell ausgeführte Prüfung) auf diese Option.

4.1.1 Viren- und Spyware-Schutz

Der Viren- und Spyware-Schutz bietet durch Überwachung der Dateiaktivitäten, der E-Mail- und Internet-Kommunikation Schutz vor bösartigen Systemangriffen. Wird eine Bedrohung durch Schadcode erkannt, kann das Virenschutz-Modul den Code unschädlich machen, indem es zunächst die Ausführung des Codes blockiert und dann den Code entfernt bzw. die Datei löscht oder in die Quarantäne verschiebt.

Über die Einstellungen für Prüfungen der verschiedenen Schutzmodule (Echtzeit-Dateischutz, Web-Schutz usw.) können Sie die Erkennung folgender Elemente aktivieren und deaktivieren:

- **Evtl. unerwünschte Anwendungen** sind Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, aber auf Leistung und Verhalten Ihres Computers negative Auswirkungen haben können.
  Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

- **Potenziell unsichere Anwendungen** stellen gewerbliche Software dar, die zu einem böswilligen Zweck missbraucht werden kann. Beispiele für potenziell unsichere Anwendungen sind Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden). Diese Option ist in der Voreinstellung deaktiviert.
  Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar.

- **Verdächtige Anwendungen** umfassen Programme, die mit Packprogrammen oder Schutzprogrammen komprimiert wurden. Diese Schutzarten werden oft von Verfassern von Schadcode eingesetzt, um die Erkennung zu umgehen.

Die Anti-Stealth-Technologie ist ein fortschrittliches System zur Erkennung gefährlicher Programme wie Rootkits, die sich vor dem Betriebssystem verstecken können. Aus diesem Grund ist es nahezu unmöglich, sie mit herkömmlichen Prüfmethoden zu erkennen.

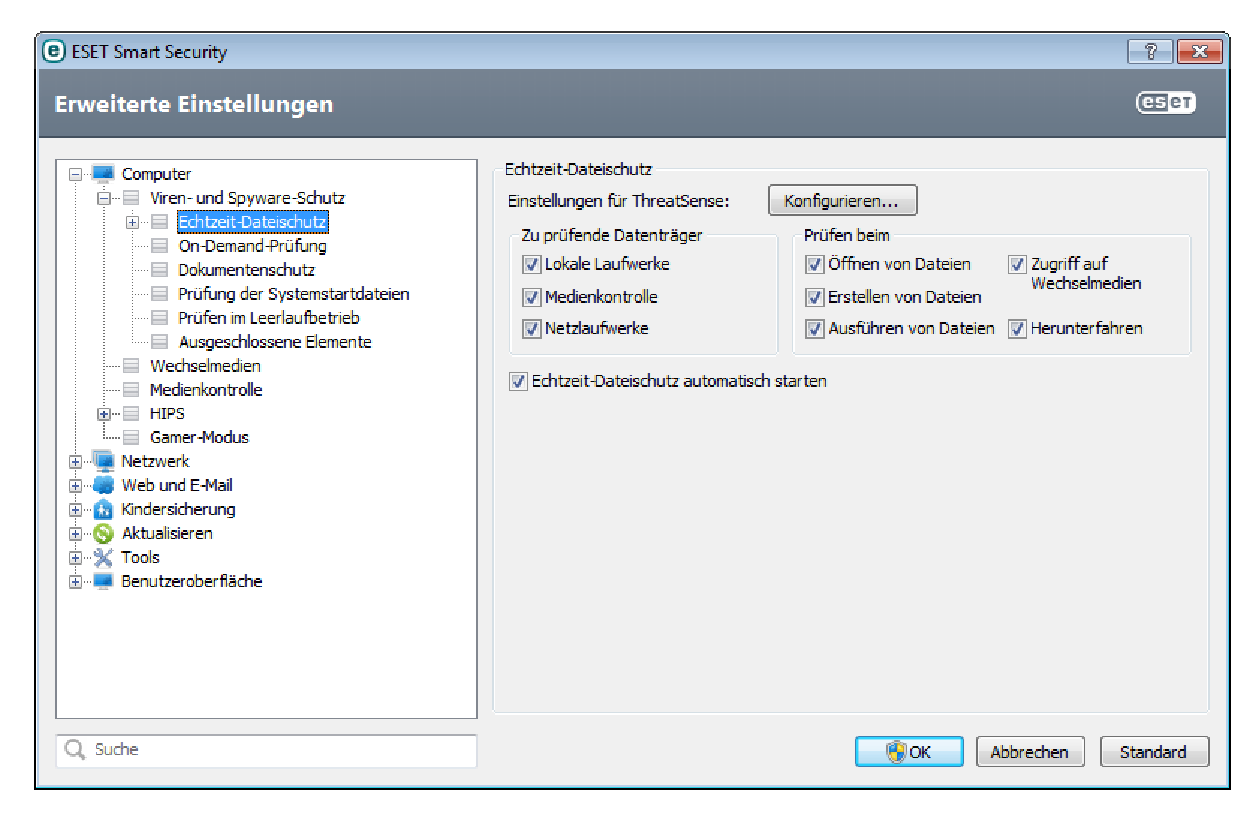
4.1.1.1 Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle für den Virenschutz relevanten Systemereignisse. Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft. Der Echtzeit-Dateischutz wird beim Systemstart gestartet.

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse wie den Zugriff auf eine Datei. Durch die Verwendung der ThreatSense-Erkennungsmethoden (siehe Abschnitt Einstellungen für ThreatSense) kann der Echtzeit-Dateischutz so konfiguriert werden, dass neu erstellte und vorhandene Dateien unterschiedlich behandelt werden. Sie können den Echtzeit-Dateischutz z. B. so konfigurieren, dass neuere Dateien genauer überwacht werden.

Bereits geprüfte Dateien werden nicht erneut geprüft (sofern sie nicht geändert wurden), um die Systembelastung durch den Echtzeit-Dateischutz möglichst gering zu halten. Nach einem Update der Signaturdatenbank werden die Dateien sofort wieder geprüft. Mit der **Smart-Optimierung** legen Sie die Prüfeinstellungen fest. Wenn diese Option deaktiviert ist, werden alle Dateien bei jedem Zugriff geprüft. Um die Option zu ändern, klicken Sie in dem Fenster mit den erweiterten Einstellungen **F5** auf **Computer** > **Viren- und Spyware-Schutz** > **Echtzeit-Dateischutz**. Klicken Sie auf **Einstellungen...** neben **ThreatSense-Einstellungen**> **Sonstige** und aktivieren bzw. deaktivieren Sie die Option **Smart-Optimierung aktivieren**.

Der Echtzeit-Dateischutz wird standardmäßig beim Systemstart gestartet und fortlaufend ausgeführt. In Ausnahmefällen (z. B. bei einem Konflikt mit einer anderen Echtzeitprüfung) kann der Echtzeit-Dateischutz deaktiviert werden. Wählen Sie dazu die Option **Echtzeit-Dateischutz automatisch starten** im Bereich **Echtzeit-Dateischutz** in den erweiterten Einstellungen.



Zu prüfende Datenträger

In der Standardeinstellung werden alle Datenträger auf mögliche Bedrohungen geprüft:

Lokale Laufwerke - Geprüft werden alle lokalen Laufwerke
Medienkontrolle - CD/DVDs, USB-Speicher, Bluetooth-Geräte, usw.
Netzlaufwerke - Geprüft werden alle zugeordneten Netzlaufwerke

Es wird empfohlen, diese Einstellungen nur in Ausnahmefällen zu ändern, z. B. wenn die Prüfung bestimmter Datenträger die Datenübertragung deutlich verlangsamt.

Prüfen bei (ereignisgesteuerte Prüfung)

Standardmäßig werden alle Dateien beim Öffnen, Erstellen und Ausführen geprüft. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. So bietet der Echtzeit-Dateischutz auf Ihrem Computer maximale Sicherheit:

- **Öffnen von Dateien** - Prüfen von Dateien beim Öffnen aktivieren/deaktivieren.
- **Erstellen von Dateien** - Prüfen von Dateien beim Erstellen oder Ändern aktivieren/deaktivieren.
- **Ausführen von Dateien** - Prüfen von Dateien beim Ausführen aktivieren/deaktivieren.
- **Wechselmedienzugriff** - Prüfen beim Zugriff auf Wechselmedien mit Speicherplatz aktivieren/deaktivieren.
- **Computer-Abschaltung** - Prüfen beim Herunterfahren des Computers aktivieren/deaktivieren.

4.1.1.1.1 Erweiterte Optionen für Prüfungen

Detailliertere Einstellungsoptionen finden Sie unter **Computer** > **Viren- und Spyware-Schutz** > **Echtzeit-Dateischutz** > **Erweiterte Einstellungen**.

Zusätzliche ThreatSense-Einstellungen für neu erstellte und geänderte Dateien - Das Infektionsrisiko für neu erstellte oder geänderte Dateien ist vergleichsweise größer als für vorhandene Dateien. Daher prüft das Programm solche Dateien mit zusätzlichen Parametern. Zusätzlich zu den üblichen Prüfmethoden auf Signaturbasis wird die Advanced Heuristik verwendet. Diese Methode erkennt neue Bedrohungen, bevor ein Update der Signaturdatenbank veröffentlicht wird. Neben neu erstellten Dateien werden auch selbstentpackende Archive (SFX) und laufzeitkomprimierte Dateien (intern komprimierte, ausführbare Dateien) geprüft. In den Standardeinstellungen werden Archive unabhängig von ihrer eigentlichen Größe bis zur 10. Verschachtelungsebene geprüft. Deaktivieren Sie die Option **Standard-Archivprüfeinstellungen**, um die Archivprüfeinstellungen zu ändern.

Zusätzliche ThreatSense-Einstellungen für ausführbare Dateien - Standardmäßig wird bei der Dateiausführung keine Advanced Heuristik verwendet. Unter Umständen kann es jedoch sinnvoll sein, diese Option zu aktivieren.

(über das Kontrollkästchen **Advanced Heuristik bei Dateiausführung**). Beachten Sie, dass die Advanced Heuristik die Ausführung einiger Programme aufgrund erhöhter Systemanforderungen verlangsamen kann. Wenn die Option **Advanced Heuristik bei der Ausführung von Dateien auf Wechselmedien** aktiviert ist, Sie aber einige Anschlüsse für Wechselmedien (USB-Anschlüsse) von der Prüfung durch die Advanced Heuristik bei Dateiausführung ausschließen möchten, klicken Sie auf **Ausnahmen**, um das Dialogfenster für Ausschlüsse von Wechselmedien zu öffnen. In diesem Fenster können Sie die Einstellungen ändern, indem Sie das Kontrollkästchen des entsprechenden Anschlusses aktivieren bzw. deaktivieren.

4.1.1.1.2 Säuberungsstufen

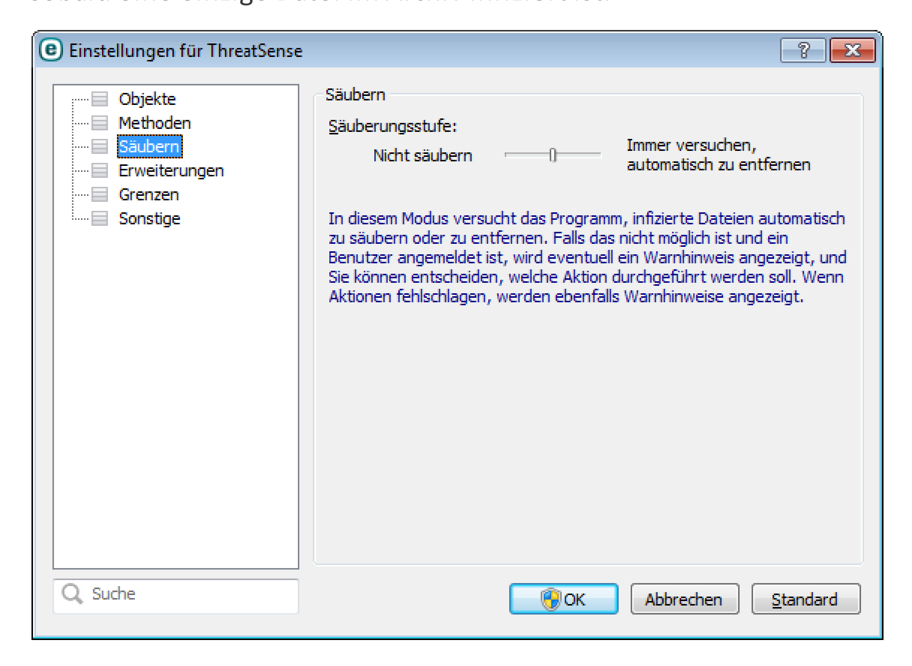
Für den Echtzeit-Dateischutz stehen drei Säuberungsstufen zur Verfügung (unter **Einstellungen** im Bereich **Echtzeit-Dateischutz** unter **Säubern**).

Nicht säubern - Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und der Benutzer wird aufgefordert, eine Aktion auszuwählen. Diese Stufe eignet sich für fortgeschrittene Benutzer, die wissen, wie sie im Falle eingedrungener Schadsoftware vorgehen sollen.

Normales Säubern - Das Programm versucht, infizierte Dateien automatisch zu säubern oder zu löschen. Es wendet hierzu vordefinierte Aktionen an (je nach Art der Infiltration). Ein Hinweis am unteren rechten Bildschirmrand informiert über die Erkennung und das Löschen infizierter Dateien. Wenn es nicht möglich ist, die angemessene Aktion automatisch zu bestimmen, schlägt das Programm verschiedene Aktionen vor. Dies gilt auch für Fälle, in denen eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden kann.

Immer versuchen, automatisch zu säubern - Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien. Ausnahmen gelten nur für Systemdateien. Wenn es nicht möglich ist, den Schadcode zu entfernen, wird der Benutzer aufgefordert, eine Aktion auszuwählen.

Warnung: Wenn infizierte Dateien in einem Archiv gefunden werden, sind zwei Vorgehensweisen möglich. Im Standardmodus („normales Säubern“) wird die Archivdatei nur dann gelöscht, wenn alle Dateien im Archiv infiziert sind. Wenn die Option **Immer versuchen, automatisch zu entfernen** aktiviert ist, wird die Archivdatei gelöscht, sobald eine einzige Datei im Archiv infiziert ist.



4.1.1.1.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Dateischutz ist die wichtigste Komponente für ein sicheres System. Daher sollte gründlich geprüft werden, ob eine Änderung der Einstellungen wirklich notwendig ist. Es wird empfohlen, seine Parameter nur in einzelnen Fällen zu verändern.

Bei der Installation von ESET Smart Security werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Zum Wiederherstellen der Standardeinstellungen klicken Sie auf **Standard** in der unteren rechten Ecke des Fensters **Echtzeit-Dateischutz** (**Erweiterte Einstellungen** > **Computer** > **Viren- und Spyware-Schutz** > **Echtzeit-Dateischutz**).

4.1.1.1.4 Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz aktiv ist und Viren erkennt, verwenden Sie eine Testdatei von eicar.com. Diese Testdatei ist harmlos und wird von allen Virenschutzprogrammen erkannt. Die Datei wurde von der Firma EICAR (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen. Die Datei kann unter http://www.eicar.org/download/eicar.com heruntergeladen werden.

HINWEIS: Bevor Sie eine Prüfung des Echtzeit-Dateischutzes durchführen, müssen Sie die Firewall deaktivieren. Bei aktivierter Firewall wird die Datei erkannt, und die Testdateien können nicht heruntergeladen werden.

4.1.1.1.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

In diesem Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

Echtzeit-Dateischutz ist deaktiviert

Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Dateischutz erneut zu aktivieren, klicken Sie auf **Einstellungen** und dann auf den Bereich **Echtzeit-Dateischutz** im Hauptprogrammfenster.

Wenn der Echtzeit-Dateischutz beim Systemstart nicht gestartet wird, ist wahrscheinlich die Option **Echtzeit-Dateischutz automatisch starten** deaktiviert. Zum Aktivieren dieser Option klicken Sie in den erweiterten Einstellungen (**F5**) auf **Computer** > **Viren- und Spyware-Schutz** > **Echtzeit-Dateischutz**. Aktivieren Sie im Bereich **Erweiterte Einstellungen** am unteren Rand des Fensters das Kontrollkästchen **Echtzeit-Dateischutz automatisch starten**.

Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode

Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Schutzprogramme können miteinander in Konflikt geraten. Wir empfehlen Ihnen, vor der Installation von ESET alle anderen Virusschutzprogramme zu deinstallieren.

Echtzeit-Dateischutz startet nicht

Wenn der Echtzeit-Dateischutz beim Systemstart nicht initialisiert wird (und die Option **Echtzeit-Dateischutz automatisch starten** aktiviert ist), kann dies an Konflikten mit anderen Programmen liegen. Sollte dies der Fall sein, wenden Sie sich an den ESET-Support.

4.1.1.2 Computer prüfen

Die manuelle Prüfung ist ein wichtiger Teil Ihrer Virenschutzlösung. Sie dient zur Prüfung von Dateien und Ordnern auf dem Computer. Aus Sicherheitsgründen ist es dringend erforderlich, dass Sie Ihren Computer nicht nur bei Infektionsverdacht prüfen, sondern diese Prüfung in die allgemeinen Sicherheitsroutinen integrieren. Es wird empfohlen, regelmäßig eine umfassende Prüfung des Computers vorzunehmen, um Viren zu entdecken, die nicht vom Echtzeit-Dateischutz erfasst wurden, als sie auf die Festplatte gelangten. Dies kommt z. B. vor, wenn der Echtzeit-Dateischutz zu diesem Zeitpunkt deaktiviert oder die Signaturdatenbank nicht auf dem neuesten Stand war oder die Datei nicht als Virus erkannt wurde.

Die hierfür vorgesehene Funktion **Computer prüfen** hat zwei Unterbefehle. Bei der **Smart-Prüfung** wird das System schnell überprüft, ohne dass Sie dafür weitere Prüfparameter konfigurieren müssen. Unter **Prüfen mit speziellen Einstellungen** können Sie eines der vordefinierten Prüfprofile für bestimmte Speicherorte auswählen oder bestimmte zu prüfende Objekte festlegen.

Smart-Prüfung

Mit der Smart-Prüfung können Sie schnell den Computer prüfen und infizierte Dateien säubern, ohne eingreifen zu müssen. Ihr Vorteil ist die einfache Bedienung, bei der Sie keine detaillierten Prüfeinstellungen festlegen müssen. Bei der Smart-Prüfung werden alle Dateien auf allen Laufwerken geprüft, und erkannte eingedrungene Schadsoftware wird automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungstypen finden Sie unter Säubern.

Prüfen mit speziellen Einstellungen

Beim Prüfen mit speziellen Einstellungen können Sie verschiedene Prüfparameter festlegen, z. B. die zu prüfenden Objekte und die Prüfmethoden. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Verschiedene Konfigurationen können in benutzerdefinierten Prüfprofilen gespeichert werden. Das ist sinnvoll, wenn Prüfungen wiederholt mit denselben Parametern ausgeführt werden.

Prüfen von Wechselmedien

Diese Prüfung ähnelt der Smart-Prüfung und ermöglicht ein schnelles Prüfen der aktuell an den Computer angeschlossenen Wechselmedien (wie CD/DVD/USB). Diese Prüfung ist hilfreich, wenn Sie beispielsweise ein USB-Speichergerät an den Computer anschließen und den Inhalt auf Schadcode und sonstige mögliche Bedrohungen untersuchen möchten.

Sie können diese Prüfung auch über **Prüfen mit speziellen Einstellungen** starten, indem Sie im Dropdown-Menü **Zu prüfende Objekte** den Eintrag **Wechselmedien** auswählen und auf **Prüfen** klicken.

Weitere Informationen zum Prüfprozess finden Sie im Abschnitt Stand der Prüfung.

Sie sollten mindestens einmal im Monat eine Prüfung des Computers vornehmen. Sie können die Prüfung als Task unter **Tools** > **Taskplaner** konfigurieren.

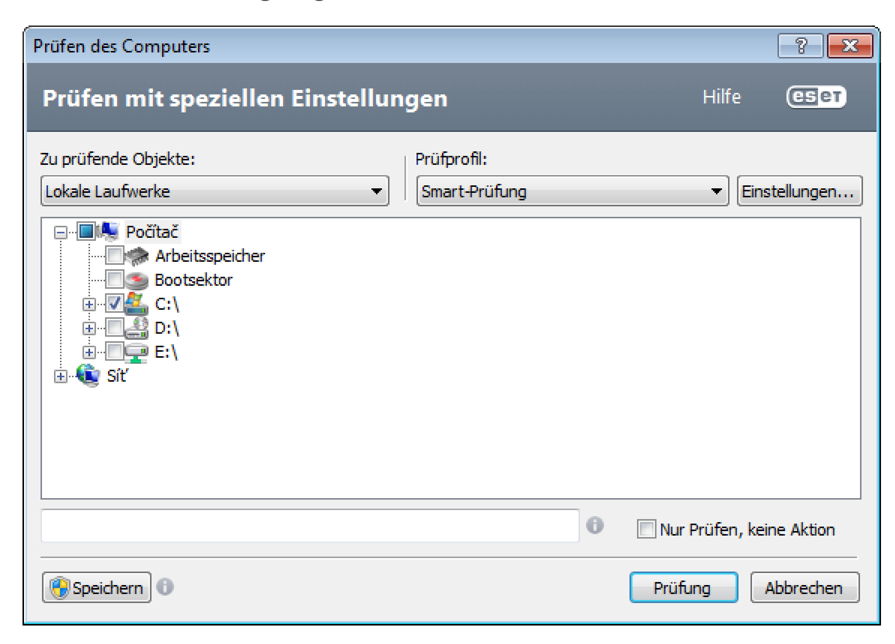
4.1.1.2.1 Prüfen mit speziellen Einstellungen

Wenn Sie nicht den gesamten Festplattenspeicher, sondern nur bestimmte Objekte prüfen möchten, klicken Sie auf **Computer prüfen** > **Prüfen mit speziellen Einstellungen**. Wählen Sie die zu prüfenden Objekte aus dem Dropdown-Menü **Zu prüfende Objekte** oder in der Ordnerstruktur (Baumstruktur) aus.

Im Fenster der zu prüfenden Objekte können Sie definieren, welche Objekte (Arbeitsspeicher, Laufwerke, Dateien und Ordner) auf Infiltrationen geprüft werden. Wählen Sie die zu prüfenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden. Im Dropdown-Menü **Zu prüfende Objekte** können Sie vordefinierte Optionen für die zu prüfenden Objekte auswählen.

- **Nach Profileinstellungen** - Im Profil festgelegte Prüfziele
- **Wechselmedien** - Disketten, USB-Speichergeräte, CDs/DVDs
- **Lokale Laufwerke** - Alle lokalen Systemlaufwerke
- **Netzlaufwerke** - Alle zugeordneten Netzlaufwerke
- **Keine Auswahl** - Bricht die Zielauswahl ab

Um schnell zu einem zu prüfenden Objekt zu navigieren oder um ein gewünschtes Objekt (Ordner oder Datei(ein)) direkt hinzuzufügen, geben Sie den Pfad in das leere Textfeld unter der Ordnerliste ein. Dies ist nur möglich, wenn keine Objekte aus der Baumstruktur zur Prüfung ausgewählt wurden und im Menü **Zu prüfende Objekte** die Option **Keine Auswahl** festgelegt ist.



Infizierte Objekte werden nicht automatisch gesäubert. Durch das Durchführen einer Prüfung ohne Aktion können Sie sich einen Eindruck des aktuellen Schutzstatus verschaffen. Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion**. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen** > **Säubern**. Die Informationen zur Prüfung werden in einem Log gespeichert.

Aus dem Dropdown-Menü **Prüfprofil** können Sie ein Profil auswählen, um ausgewählte Objekte zu prüfen. Das Standardprofil ist **Smart-Prüfung**. Es stehen außerdem zwei weitere vordefinierte Prüfprofile zur Verfügung: **Tiefenprüfung** und **Kontextmenü-Prüfung**. Diese Prüfprofile verwenden unterschiedliche ThreatSense-Einstellungen. Klicken Sie auf **Einstellungen...**, um ein ausgewähltes Prüfprofil detailliert zu konfigurieren. Die verfügbaren Optionen werden in Einstellungen für Prüfung beschrieben.

Klicken Sie auf **Speichern**, um die an den zu prüfenden Objekten vorgenommenen Änderungen zu speichern, einschließlich der Auswahl in der Baumstruktur.

Klicken Sie auf **Prüfen**, um die Prüfung mit den von Ihnen festgelegten Parametern auszuführen.

Mit der Schaltfläche Als Administrator prüfen können Sie die Prüfung mit dem Administratorkonto ausführen. Wählen Sie diese Option, wenn der aktuell angemeldete Benutzer keine ausreichenden Zugriffsrechte auf die zu prüfenden Dateien hat. Diese Schaltfläche ist nur verfügbar, wenn der aktuell angemeldete Benutzer UAC-

Vorgänge als Administrator aufrufen kann.

4.1.1.2.2 Stand der Prüfung

Die Fortschrittsanzeige enthält den aktuellen Stand der Prüfung sowie die Anzahl der bisher gefundenen infizierten Dateien.

HINWEIS: Es ist normal, dass u. a. passwortgeschützte Dateien oder Dateien, die ausschließlich vom System genutzt werden (in der Regel sind das *pagefile.sys* und bestimmte Log-Dateien), nicht geprüft werden können.

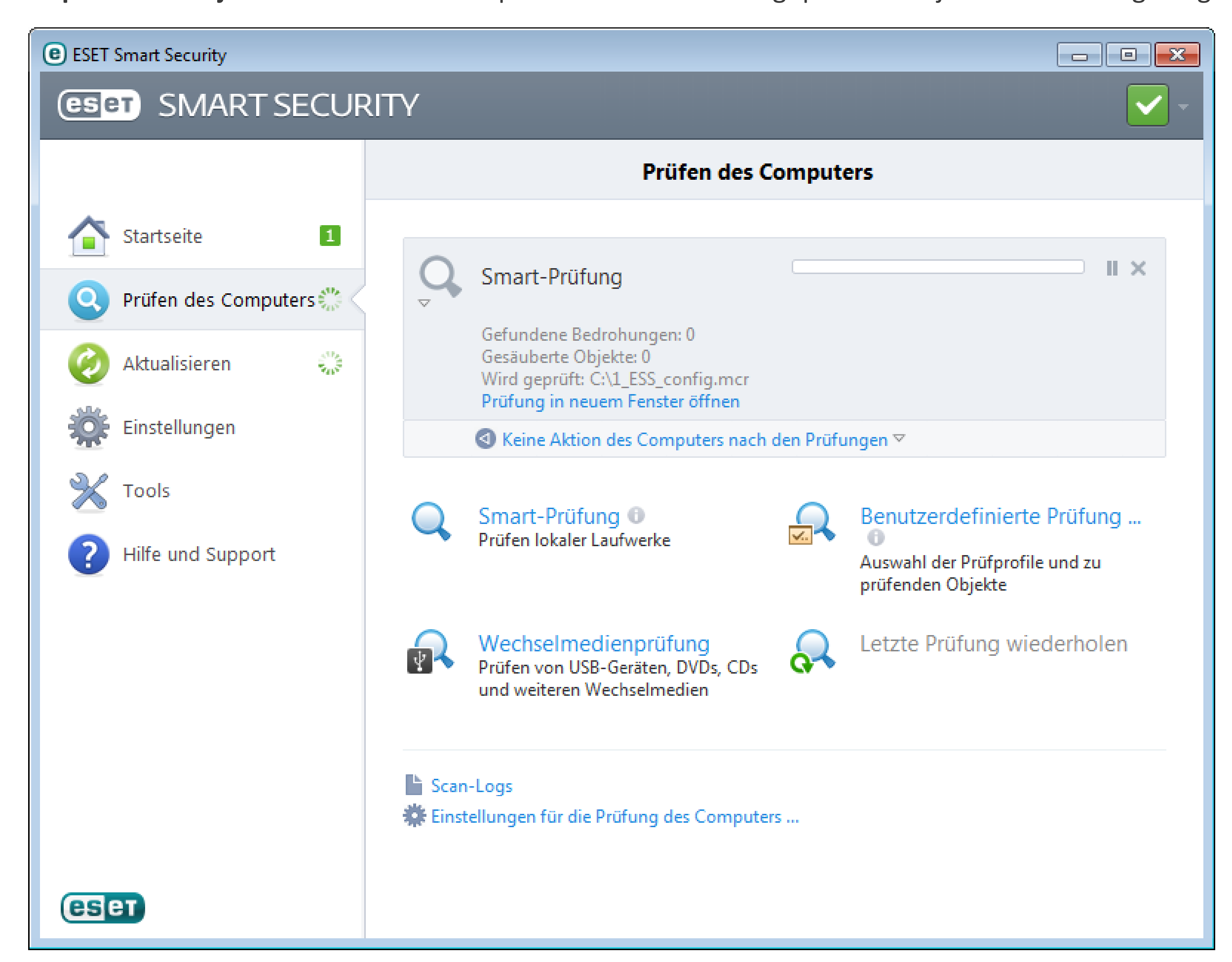
Die Fortschrittsanzeige zeigt den Prozentsatz der bereits geprüften Objekte in Bezug auf die noch zu prüfenden Objekte an. Dieser Wert ergibt sich aus der Gesamtzahl der Objekte, die in die Prüfung einbezogen werden.

Tipps

Klicken Sie auf die Lupe oder den Pfeil, um Details zur aktuell ausgeführten Prüfung anzuzeigen.
Sie können gleichzeitig eine weitere Prüfung ausführen, indem Sie auf **Smart-Prüfung** oder **Prüfen mit speziellen Einstellungen** klicken.

Objekte - Zeigt die Gesamtzahl der während der Prüfung geprüften Dateien, gefundenen Bedrohungen und gesäuberten Bedrohungen an.

Zu prüfende Objekte - Der Name und Speicherort des aktuell geprüften Objekts werden angezeigt.



Keine Aktion des Computers nach den Prüfungen - Löst ein geplantes Herunterfahren oder einen geplanten Neustart des Computers nach der Prüfung aus. Nach dem Abschluss der Prüfung wird vor dem Herunterfahren 60 Sekunden lang ein Bestätigungsfenster angezeigt. Klicken Sie erneut auf die Option, um die ausgewählte Aktion zu deaktivieren.

4.1.1.2.3 Prüfprofile

Ihre bevorzugten Einstellungen können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

Um ein neues Profil zu erstellen, öffnen Sie das Fenster mit den erweiterten Einstellungen (F5) und klicken Sie auf **Computer** > **Viren- und Spyware-Schutz** > **On-Demand-Prüfung** > **Profile...**. Im Fenster **Konfigurationsprofile** befindet sich das Dropdown-Menü **Ausgewähltes Profil** mit den vorhandenen Prüfprofilen und der Option zum Erstellen eines neuen Profils. Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt Einstellungen für ThreatSense. So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Beispiel: Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Smart-Prüfung eignet sich in gewissem Maße, aber Sie möchten nicht die laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option **Immer versuchen, automatisch zu entfernen** anwenden. Klicken Sie im Fenster **Konfigurationsprofile** auf **Hinzufügen...**. Geben Sie den Namen des neuen Profils im Feld **Profilname** ein und wählen Sie im Dropdown-Menü **Einstellungen kopieren von Profil** die Option **Smart-Prüfung**. Passen Sie anschließend die übrigen Parameter Ihren eigenen Erfordernissen an und speichern Sie Ihr neues Profil.

4.1.1.3 Prüfung der Systemstartdateien

Die automatische Prüfung der Systemstartdateien wird standardmäßig beim Systemstart und beim Update der Signaturdatenbank ausgeführt. Die Ausführung der Prüfung ist abhängig davon, wie der Taskplaner konfiguriert ist und welche Tasks eingerichtet wurden.

Die Option der Systemstartprüfung ist Bestandteil der Task **Prüfung der Systemstartdateien** im Taskplaner. Navigieren Sie zum Ändern der Einstellungen nach **Tools** > **Taskplaner** und klicken Sie auf **Prüfung Systemstartdateien** und anschließend auf **Bearbeiten...**. Nach dem letzten Schritt wird das Fenster Prüfung Systemstartdateien angezeigt. (Weitere Informationen finden Sie im nächsten Kapitel.)

Detaillierte Anweisungen zum Erstellen und Verwalten von Tasks im Taskplaner finden Sie unter Erstellen neuer Tasks.

4.1.1.3.1 Prüfung Systemstartdateien

Beim Erstellen eines geplanten Tasks für die Prüfung der Systemstartdateien stehen Optionen zum Anpassen der folgenden Parameter zur Verfügung:

Im Dropdownmenü **Prüfstufe** können Sie die Prüftiefe für Dateien festlegen, die beim Systemstart ausgeführt werden. Die Dateien werden auf Grundlage der folgenden Kriterien in aufsteigender Reihenfolge sortiert:

- **Nur die am häufigsten verwendeten Dateien** (kleinste Anzahl geprüfter Dateien)
- **Häufig verwendete Dateien**
- **Von den meisten Benutzern verwendete Dateien**
- **Selten verwendete Dateien**
- **Alle registrierten Dateien** (größte Anzahl geprüfter Dateien)

Außerdem stehen zwei **Prüfstufen**-Gruppen zur Verfügung:

- **Dateien, die vor der Benutzeranmeldung gestartet werden** - Enthält Dateien von Standorten, auf die ohne Benutzeranmeldung zugegriffen werden kann (umfasst nahezu alle Systemstartstandorte wie Dienste, Browserhilfsobjekte, Windows-Anmeldungshinweise, Einträge im Windows-Taskplaner, bekannte DLL-Dateien usw.).
- **Dateien, die nach der Benutzeranmeldung gestartet werden** - Enthält Dateien von Standorten, auf die erst nach einer Benutzeranmeldung zugegriffen werden kann (umfasst Dateien, die nur für einen bestimmten Benutzer ausgeführt werden, üblicherweise im Verzeichnis *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows \CurrentVersion\Run*).

Die Liste der zu prüfenden Dateien ist für jede der zuvor genannten Gruppen unveränderbar.

Prüfpriorität - Die Priorität, mit der der Prüfbeginn ermittelt wird:

- **Normal** - bei durchschnittlicher Systemlast
- **Niedrig** - bei geringer Systemlast
- **Minimal** - bei minimaler Systemlast
- **Bei Leerlauf** - Der Task wird nur ausgeführt, wenn das System im Leerlauf ist.

4.1.1.4 Prüfen im Leerlaufbetrieb

Die Prüfung im Leerlaufbetrieb kann in den **erweiterten Einstellungen** unter **Computer** > **Viren- und Spyware-Schutz** > **Prüfen im Leerlaufbetrieb** aktiviert werden. Wenn der Computer im Leerlauf ist, wird auf allen lokalen Festplatten eine Prüfung ausgeführt. unter Auslöser für die Prüfung im Leerlaufbetrieb finden Sie eine Liste der Bedingungen, die die Prüfung im Leerlaufbetrieb auslösen.

Diese Prüfung wird nur dann ausgeführt, wenn der Computer (Notebook) an die Netzversorgung angeschlossen ist. Sie können diese Einstellung überschreiben, indem Sie das Kontrollkästchen neben **Auch ausführen, wenn der Computer im Batteriebetrieb ausgeführt wird** in den erweiterten Einstellungen aktivieren.

Wählen Sie **Erstellen von Logs aktivieren** in den erweiterten Einstellungen, um die Ausgabe einer Computerprüfung in den Log-Dateien abzulegen (Klicken Sie im Hauptprogrammfenster auf **Tools** > **Log-Dateien** und wählen Sie **Prüfen des Computers** im Dropdown-Menü **Log** aus).

Die letzte Einstellung in diesem Abschnitt betrifft ThreatSense. Klicken Sie auf **Konfigurieren...**, wenn Sie mehrere Prüfparameter (z. B. Erkennungsmethoden) ändern möchten.

4.1.1.5 Ausschlussfilter

Mit dem Ausschlussfilter können Sie festlegen, welche Dateien und Ordner von Prüfungen ausgenommen werden sollen. Um zu gewährleisten, dass möglichst alle Objekte auf Bedrohungen geprüft werden, empfehlen wir, nur bei dringendem Bedarf Ausnahmen zu erstellen. In bestimmten Fällen kann es jedoch erforderlich sein, ein Objekt von der Prüfung auszuschließen, beispielsweise bei großen Datenbankeinträgen, deren Prüfung die Computerleistung zu stark beeinträchtigen würde, oder bei Software, die Konflikte mit der Prüfung verursacht.

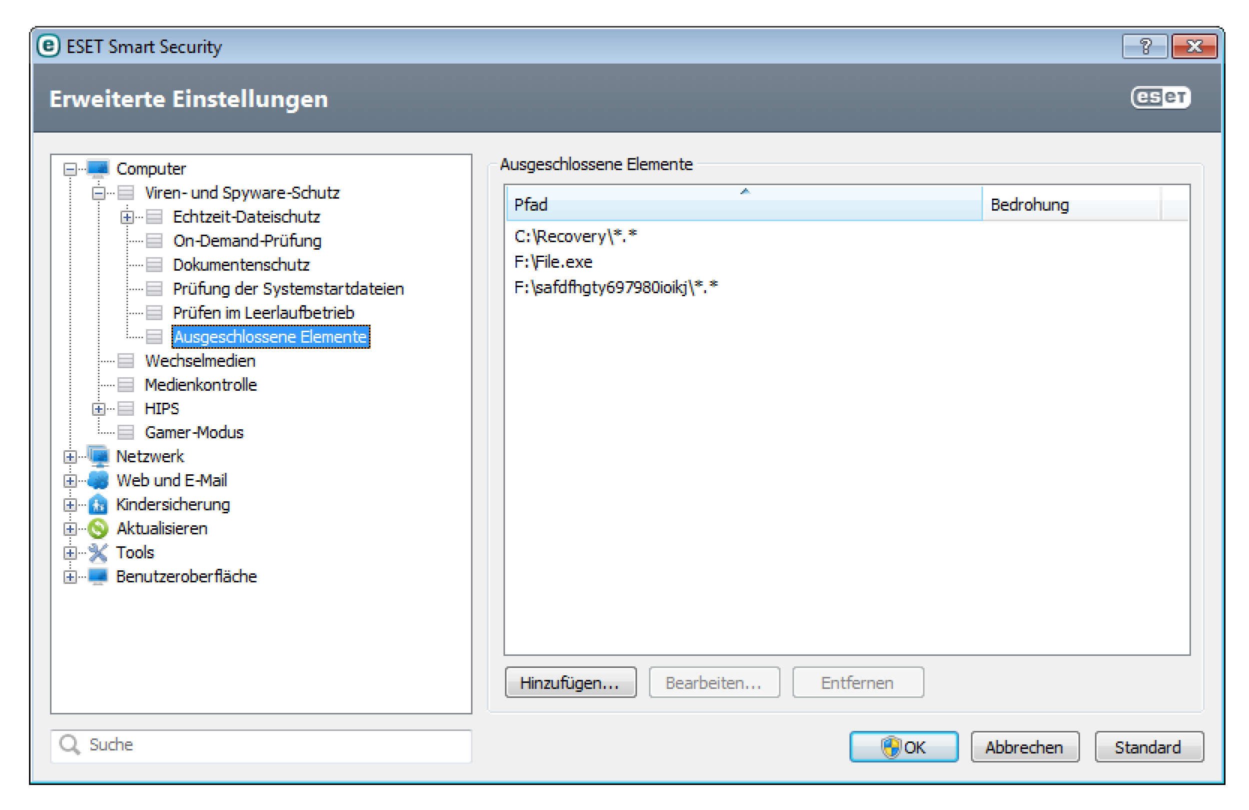
So schließen Sie ein Objekt von Prüfungen aus:

1. Klicken Sie auf **Hinzufügen...**.
2. Geben Sie den Pfad des Objekts ein oder wählen Sie es in der Baumstruktur aus.

Mit Hilfe von Platzhaltern können Sie Gruppen von Dateien ausschließen. Dabei steht ein Fragezeichen (?) für genau ein beliebiges Zeichen, ein Sternchen (*) steht für beliebig viele Zeichen oder „kein Zeichen“.

Beispiele

- Wenn Sie alle Dateien in einem bestimmten Ordner ausschließen möchten, geben Sie den Pfad zum Ordner mit der Maske „*.*“ ein.
- Wenn Sie ein gesamtes Laufwerk einschließlich aller Dateien und Unterordner ausschließen möchten, geben Sie den Pfad mit der Maske „D:*“ ein.
- Wenn nur DOC-Dateien ausgeschlossen werden sollen, verwenden Sie die Maske „*.doc“.
- Wenn der Name einer ausführbaren Datei aus einer bestimmten Anzahl von Zeichen (und diese variieren) besteht und Sie nur den ersten sicher wissen (zum Beispiel „D“), verwenden Sie folgendes Format: „D????.exe“. Die Fragezeichen ersetzen die fehlenden (unbekannten) Zeichen.



Hinweis: Eine Bedrohung, die sich in einer Datei befindet, die die Kriterien des Ausschlussfilters erfüllt, kann vom Echtzeit-Dateischutz und bei der Prüfung des Computers nicht erkannt werden.

Pfad - Pfad zu den auszuschließenden Dateien/Ordnern

Bedrohung - Steht neben einer ausgeschlossenen Datei der Name einer Bedrohung, so gilt die Ausnahme nicht generell für die Datei, sondern nur für diese bestimmte Bedrohung. Wird die Datei später durch andere Malware infiziert, erkennt der Virenschutz dies. Dieser Ausschlusstyp kann nur bei bestimmten Infiltrationsarten verwendet werden und wird entweder im Warnungsfenster für die Bedrohung erstellt (klicken Sie auf **Erweiterte Einstellungen anzeigen** und dann auf **Von der Erkennung ausschließen**) oder indem Sie unter **Einstellungen** > **Quarantäne** mit der rechten Maustaste auf die Datei in der Quarantäne klicken und aus dem Kontextmenü den Befehl **Wiederherstellen und von der Erkennung ausschließen** auswählen.

Hinzufügen... - Objekte von der Prüfung ausnehmen

Bearbeiten... - Ausgewählten Eintrag bearbeiten

Entfernen - Ausgewählten Eintrag löschen

4.1.1.6 Einstellungen für ThreatSense

ThreatSense ist eine Technologie, die verschiedene Methoden zur Erkennung von Bedrohungen verwendet. Die Technologie arbeitet proaktiv, d. h. sie schützt das System auch während der ersten Ausbreitung eines neuen Angriffs. Eingesetzt wird eine Kombination aus Code-Analyse, Code-Emulation, allgemeinen Signaturen und Virussignaturen verwendet, die zusammen die Systemsicherheit deutlich erhöhen. Das Prüfmodul kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch erfolgreich Rootkits.

in den Einstellungen für ThreatSense können Sie verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die geprüft werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

Um das Fenster für die Einstellungen zu öffnen, klicken Sie auf die Schaltfläche **Einstellungen...**, die im Fenster mit erweiterten Einstellungen für alle Module angezeigt wird, die ThreatSense verwenden (siehe unten). Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Dies sollte bei den individuellen ThreatSense-Einstellungen für die folgenden Schutzmodule berücksichtigt werden:

- Echtzeit-Dateischutz,
- Dokumentenschutz,
- E-Mail-Client-Schutz,
- Web-Schutz,
- Prüfen des Computers.

Die ThreatSense-Parameter sind für jedes Modul optimal eingerichtet. Eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Modul „Echtzeit-Dateischutz" dazu führen, dass das System langsamer arbeitet (normalerweise werden mit diesen Methoden nur neu erstellte Dateien geprüft). Es wird empfohlen, die Standard-Parameter für ThreatSense in allen Modulen unverändert beizubehalten. Änderungen sollten nur im Modul „Computer prüfen" vorgenommen werden.

4.1.1.6.1 Objekte

Im Bereich **Objekte** können Sie festlegen, welche Dateien und Komponenten Ihres Computers auf Schadcode geprüft werden sollen.

Arbeitsspeicher - Prüfung auf Bedrohungen für den Arbeitsspeicher des Systems.

Systembereiche (Boot, MBR) - Prüfung der Bootsektoren auf Viren im Master Boot Record.

E-Mail-Dateien - Folgende Erweiterungen werden vom Programm unterstützt: DBX (Outlook Express) und EML.

Archive - Folgende Erweiterungen werden vom Programm unterstützt: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE und viele andere.

Selbstentpackende Archive - Selbstentpackende Archive (SFX) sind Archive, die ohne externe Programme dekomprimiert werden können.

Laufzeitkomprimierte Dateien - Im Unterschied zu Standardarchiven werden laufzeitkomprimierte Dateien nach dem Starten im Arbeitsspeicher dekomprimiert. Neben statischen laufzeitkomprimierten Dateiformaten (UPX, yoda, ASPack, FSG usw.) kann das Programm durch Code-Emulation viele weitere SFX-Typen bearbeiten.

4.1.1.6.2 Methoden

Wählen Sie unter **Methoden**, mit welchen Methoden das System auf eingedrungene Schadsoftware geprüft werden soll. Folgende Optionen stehen zur Verfügung:

Heuristik - Als heuristische Methoden werden Verfahren bezeichnet, die (bösartige) Aktivitäten von Programmen analysieren. Auf diese Weise können auch bösartige Programme erkannt werden, die zuvor noch nicht existierten oder von den vorigen Signaturdatenbanken nicht identifiziert wurden. Nachteilig ist, dass es in Einzelfällen zu Fehlalarmen kommen kann.

Advanced Heuristik/DNA/Smart-Signaturen - Advanced Heuristik ist eine der Technologien, mit denen ESET Smart Security Bedrohungen proaktiv erkennen kann. Sie ist in der Lage, unbekannte Malware durch Emulation auf Basis ihrer Funktionalität zu identifizieren. Mit diesem neuen binären Übersetzer können Anti-Emulations-Tricks von Malware-Entwicklern umgangen werden. In der neuesten Version wird eine völlig neuartige Methode der Code-Emulation auf Basis von binärer Übersetzung genutzt. Mit diesem neuen binären Übersetzer können Anti-Emulations-Tricks von Malware-Entwicklern umgangen werden. Zusätzlich zu diesen Verbesserungen wurde die Prüfung auf DNA-Basis umfassend aktualisiert, um die generische Erkennung zu verbessern und genauer auf aktuelle Schadsoftware reagieren zu können.

ESET Live Grid - Der Reputations-Check von ESET stellt Informationen zu geprüften Dateien den Daten des Cloud-basierten ESET Live Grid gegenüber und steigert so die Erkennungsrate und Prüfgeschwindigkeit.

4.1.1.6.3 Säubern

Die Einstellungen zum Entfernen von Schadcode legen fest, wie beim Entfernen vorgegangen werden soll. Es gibt 3 Säuberungsstufen.

4.1.1.6.4 Erweiterungen

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt einer Datei. In diesem Abschnitt der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die geprüft werden sollen.

In der Standardeinstellung werden alle Dateien unabhängig von ihrer Erweiterung geprüft. Jede Erweiterung kann der Liste ausgeschlossener Dateien hinzugefügt werden. Ist die Option **Alle Dateien prüfen** deaktiviert, zeigt die Liste alle aktuell geprüften Dateinamens-Erweiterungen an.

Um Dateien ohne Erweiterung zu prüfen, aktivieren Sie die Option **Dateien ohne Erweiterung prüfen**. **Dateien ohne Erweiterung nicht prüfen** wird verfügbar, wenn **Alle Alle Dateien prüfen** aktiviert ist.

Der Ausschluss bestimmter Dateien ist dann sinnvoll, wenn die Prüfung bestimmter Dateitypen die Funktion eines Programms beeinträchtigt, das diese Erweiterungen verwendet. So sollten Sie z. B. die Erweiterungen EDB, EML und TMP ausschließen, wenn Sie Microsoft Exchange Server verwenden.

Über die Schaltflächen **Hinzufügen** und **Entfernen** können Sie festlegen, welche Erweiterungen geprüft werden sollen. Wenn Sie eine **Erweiterung** eingeben, wird die Schaltfläche **Hinzufügen** aktiviert. Klicken Sie auf diese Schaltfläche, um die eingegebene Erweiterung zur Liste hinzuzufügen. Wählen Sie eine Erweiterung in der Liste aus und klicken Sie auf **Entfernen**, um die markierte Erweiterung aus der Liste zu entfernen.

Sie können die Sonderzeichen „*“ (Sternchen) und „?“ (Fragezeichen) verwenden. Das Sternchen ersetzt eine beliebige Zeichenfolge, das Fragezeichen ein beliebiges Symbol. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie darauf, dass die Zeichen „*“ und „?“ korrekt verwendet werden.

Um die Erweiterungsliste auf die Standardeinstellungen zurückzusetzen, klicken Sie auf die Schaltfläche **Standard** und anschließend zur Bestätigung auf **Ja**.

4.1.1.6.5 Grenzen

Im Bereich „Grenzen“ können Sie die Maximalgröße von Elementen und Stufen verschachtelter Archive festlegen, die geprüft werden sollen:

Maximale Objektgröße - Definiert die Maximalgröße der zu prüfenden Elemente. Der aktuelle Virenschutz prüft dann nur die Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, dass größere Elemente von der Prüfung ausgeschlossen werden. Der Standardwert ist *unbegrenzt*.

Maximale Prüfzeit pro Objekt (Sek.) - Definiert die maximale Dauer für die Prüfung eines Elements. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet der Virenschutz die Prüfung eines Elements, sobald diese Zeit abgelaufen ist, und zwar ungeachtet dessen, ob die Prüfung abgeschlossen ist oder nicht. Der Standardwert ist *unbegrenzt*.

Verschachtelungstiefe bei Archiven - Legt die maximale Tiefe der Virenprüfung von Archiven fest. Der Standardwert ist *10*.

Maximalgröße von Dateien im Archiv - Hier können Sie die maximale Dateigröße für Dateien in (extrahierten) Archiven festlegen, die geprüft werden sollen. Der Standardwert ist *unbegrenzt*.

Wird die Prüfung eines Archivs aus diesen Gründen vorzeitig beendet, bleibt das Archiv ungeprüft.

Hinweis: Die Standardwerte sollten nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund.

4.1.1.6.6 Sonstige

Die folgenden Optionen können Sie im Bereich **Sonstige** konfigurieren:

Alle Objekte in Log aufnehmen - Wenn Sie diese Option aktivieren, werden alle geprüften Dateien im Log eingetragen. Es werden also auch Dateien eingetragen, bei denen keine Bedrohung erkannt wurde. Wenn beispielsweise in einem Archiv Schadcode gefunden wird, listet das Log auch die in diesem Archiv enthaltenen, nicht infizierten Dateien auf.

Smart-Optimierung aktivieren - Wenn die Smart-Optimierung aktiviert ist, werden die optimalen Einstellungen verwendet, um die effizienteste Prüfung bei höchster Geschwindigkeit zu gewährleisten. Die verschiedenen Schutzmodule führen eine intelligente Prüfung durch. Dabei verwenden sie unterschiedliche Prüfmethoden für die jeweiligen Dateitypen. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern der entsprechenden Module für die Prüfung verwendet.

Bei der Konfiguration der Einstellungen für ThreatSense zur Prüfung des Computers sind folgende Optionen verfügbar:

Alternative Datenströme (ADS) prüfen - Bei den von NTFS-Dateisystemen verwendeten alternativen Datenströmen (ADS) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Prüftechniken nicht erkannt werden können. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

Hintergrundprüfungen mit geringer Priorität ausführen - Jede Prüfung nimmt eine bestimmte Menge von Systemressourcen in Anspruch. Wenn Sie mit Anwendungen arbeiten, die die Systemressourcen stark beanspruchen, können Sie eine Hintergrundprüfung mit geringer Priorität aktivieren, um Ressourcen für die Anwendungen zu sparen.

Datum für „Geändert am“ beibehalten - Aktivieren Sie diese Option, um den Zeitpunkt des ursprünglichen Zugriffs auf geprüfte Dateien beizubehalten (z. B. für die Verwendung mit Datensicherungssystemen), anstatt ihn zu aktualisieren.

Bildlauf für Log - Mit dieser Option können Sie den Bildlauf für das Log aktivieren oder deaktivieren. Wenn der Bildlauf aktiviert ist, werden die Informationen im Anzeigefenster nach oben verschoben.

4.1.1.7 Eingedrungene Schadsoftware wurde erkannt

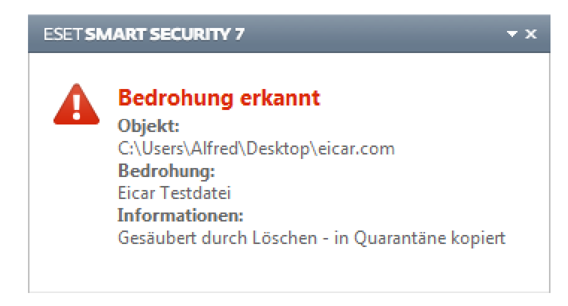
Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Eintrittsstellen sind Websites, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs, Disketten usw.).

Standardmäßiges Verhalten

ESET Smart Security kann Bedrohungen mit einem der folgenden Module erkennen:

- Echtzeit-Dateischutz
- Web-Schutz
- E-Mail-Client-Schutz
- On-Demand-Prüfung

Standardmäßig wenden die Module die normale Säuberungsstufe an und versuchen, die Datei zu säubern und in die Quarantäne zu verschieben, oder die Verbindung zu beenden. Im Infobereich der Taskleiste rechts unten auf dem Bildschirm wird ein Hinweisfenster angezeigt. Weitere Informationen zu den Säuberungsstufen und zum Verhalten des Produkts finden Sie unter Säubern.



Schadcode entfernen und löschen

Ist für den Echtzeit-Dateischutz keine vordefinierte Aktion angegeben, werden Sie in einem Warnungsfenster aufgefordert, zwischen verschiedenen Optionen zu wählen. In der Regel stehen die Optionen **Säubern**, **Löschen** und **Keine Aktion** zur Auswahl. Die Auswahl der Option **Keine Aktion** ist nicht empfehlenswert, da infizierte Dateien mit dieser Einstellung nicht gesäubert werden. Einzige Ausnahme: Sie sind sich sicher, dass die Datei harmlos ist und versehentlich erkannt wurde.



Wenden Sie die Option „Säubern“ an, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

Wenn eine infizierte Datei „gesperrt“ ist oder von einem Systemprozess verwendet wird, muss die Datei in der Regel erst freigegeben werden (häufig ist dazu ein Systemneustart erforderlich), bevor sie gelöscht werden kann.

Mehrere Bedrohungen

Falls infizierte Dateien während der Prüfung des Computers nicht gesäubert wurden (oder die Säuberungsstufe auf **Nicht säubern** festgelegt wurde), so wird ein Warnfenster angezeigt. In diesem wird danach gefragt, wie mit den Dateien verfahren werden soll. Wählen Sie Aktionen für die Dateien aus (diese werden für jede Datei in der Liste separat festgelegt). Klicken Sie dann auf **Fertig stellen**.

Dateien in Archiven löschen

Im Standard-Säuberungsmodus wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Archive, die auch nicht infizierte Dateien enthalten, werden also nicht gelöscht. Die Option „Immer versuchen, automatisch zu entfernen“ sollten Sie mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und dies unabhängig vom Status der übrigen Archivdateien.

Wenn Ihr Computer die Symptome einer Malware-Infektion aufweist (Computer arbeitet langsamer als gewöhnlich, reagiert häufig nicht usw.), sollten Sie folgendermaßen vorgehen:

- Öffnen Sie ESET Smart Security und klicken Sie auf „Computer prüfen“
- Klicken Sie auf **Smart-Prüfung** (weitere Informationen siehe Abschnitt Computer prüfen)
- Nachdem die Prüfung abgeschlossen ist, überprüfen Sie im Log die Anzahl der geprüften, infizierten und wiederhergestellten Dateien

Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, wählen Sie **Prüfen mit speziellen Einstellungen** und anschließend die Bereiche, die auf Viren geprüft werden sollen.

4.1.1.8 Dokumentenschutz

Die Dokumentenschutzfunktion überprüft Microsoft Office-Dokumente vor dem Öffnen sowie automatisch von Internet Explorer heruntergeladene Dateien wie Microsoft ActiveX-Elemente. Der Dokumentenschutz bietet eine zusätzliche Schutzebene zum Echtzeit-Dateischutz und kann deaktiviert werden, um auf Systemen, die keiner großen Anzahl an Microsoft Office-Dokumenten ausgesetzt sind, die Leistung zu verbessern.

Die Option **Systemintegration** aktiviert das Schutzmodul. Um die Option zu ändern, klicken Sie im Fenster mit den erweiterten Einstellungen (F5) in der Baumstruktur auf **Computer** > **Viren- und Spyware-Schutz** > **Dokumentenschutz**.

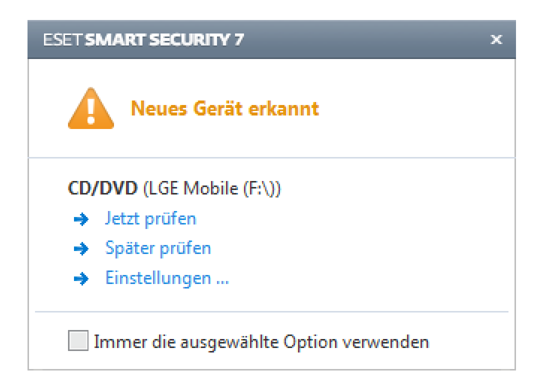
Die Funktion wird von Anwendungen aktiviert, die Microsoft Antivirus API (z. B. Microsoft Office 2000 und später oder Microsoft Internet Explorer 5.0 und später) verwenden.

4.1.2 Wechselmedien

ESET Smart Security bietet automatische Prüfmethoden für Wechselmedien (CD/DVD/USB/...). Dieses Modul ermöglicht das Einrichten einer Prüfung für eingelegte Medien. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Wechselmedien mit unerwünschten Inhalten verwenden.

Um das Verhalten einer Aktion zu ändern, die beim Anschließen eines Wechselmediums (CD/DVD/USB/...) an den Computer erfolgt, öffnen Sie mit **F5** die erweiterten Einstellungen. Erweitern Sie dann den Eintrag **Computer** zu **Viren- und Spyware-Schutz** > **Wechselmedien** und wählen Sie im Dropdown-Menü **Aktion nach Einlegen von Wechselmedien** die Standardaktion aus. Wenn die Option **Prüfoptionen anzeigen** aktiviert ist, wird ein Hinweisfenster angezeigt, in dem Sie eine Aktion wählen können:

- **Jetzt prüfen** - Eine On-Demand-Prüfung des eingelegten Wechselmediums wird durchgeführt.
- **Später prüfen** - Es wird keine Aktion ausgeführt und das Fenster **Neues Gerät erkannt** wird geschlossen.
- **Einstellungen** - Öffnet die Einstellungen für Wechselmedien.



4.1.3 Medienkontrolle

ESET Smart Security bietet Methoden zur automatischen Prüfung von Geräten (CD/DVD/USB/...). Mit diesem Modul können Sie Medien bzw. Geräte prüfen oder sperren oder erweiterte Filter- und Berechtigungseinstellungen anpassen und definieren, wie ein Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten kann. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Geräte mit unerwünschten Inhalten verwenden.

Unterstützte externe Geräte

- CD/DVD
- Datenträgerspeicher
- FireWire-Speicher

Hinweis: Wenn die Medienkontrolle in ESET Endpoint Security oder ESET Endpoint Antivirus in einer Unternehmensumgebung verwendet wird, werden zusätzliche Typen externer Geräte unterstützt.

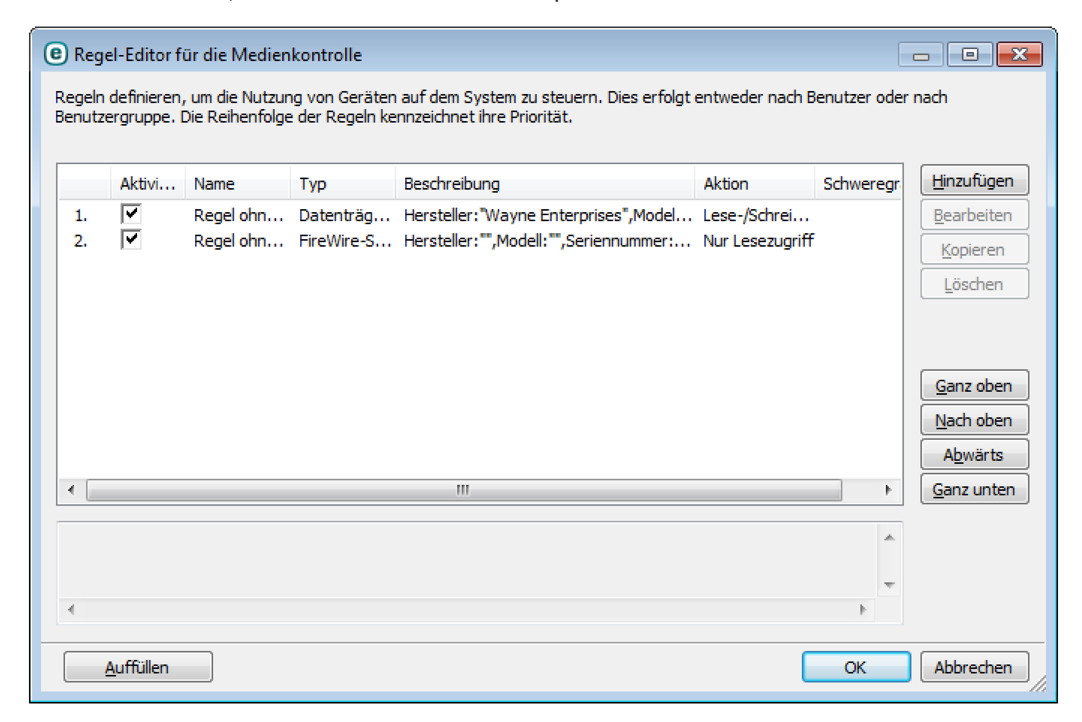
Die Einstellungen für die Medienkontrolle können unter **Erweiterte Einstellungen** (F5) > **Computer** > **Medienkontrolle** geändert werden.

Über das Kontrollkästchen **Systemintegration** aktivieren Sie die Funktion Medienkontrolle in ESET Smart Security. Sie müssen Ihren Computer neu starten, um die Änderungen zu übernehmen. Wenn die Medienkontrolle aktiviert ist, wird die Option **Regeln konfigurieren...** freigeschaltet, über die Sie das Fenster Regel-Editor für die Gerätesteuerung erreichen.

Wenn das angeschlossene externe Gerät eine vorhandene Regel anwendet, die die Aktion **Sperren** ausführt, wird in der unteren rechten Ecke ein Hinweisfenster angezeigt und der Zugriff auf das Gerät verweigert.

4.1.3.1 Regeln für die Medienkontrolle

Im Fenster **Regel-Editor für die Medienkontrolle** können Sie bestehende Regeln anzeigen und präzise Regeln für Geräte erstellen, die Benutzer an den Computer anschließen.



Bestimmte Gerätetypen können für Benutzer oder Benutzergruppen oder auf Grundlage weiterer, in der Regelkonfiguration festgelegter Parameter zugelassen oder gesperrt werden. Die Liste der Regeln enthält verschiedene Angaben wie Regelname, Art des externen Geräts, auszuführende Aktion beim Anschließen eines externen Geräts und Log-Schweregrad.

Klicken Sie zum Bearbeiten von Regeln auf **Hinzufügen** oder **Bearbeiten**. Klicken Sie auf **Kopieren**, um eine neue Regel mit vordefinierten Optionen der ausgewählten Regel zu erstellen. Die XML-Zeichenketten, die beim Klicken auf eine Regel angezeigt werden, können in den Zwischenspeicher kopiert werden, um den Systemadministrator beim Exportieren/Importieren der Daten zu unterstützen, beispielsweise für ESET Remote Administrator.

Halten Sie die Steuerungstaste (STRG) gedrückt, um mehrere Regeln auszuwählen und Aktionen (Löschen, Verschieben in der Liste) auf alle ausgewählten Regeln anzuwenden. Über das Kontrollkästchen **Aktiviert** können Sie eine Regel deaktivieren und aktivieren. Dies ist besonders dann hilfreich, wenn Sie eine Regel nicht dauerhaft löschen möchten, um sie gegebenenfalls zu einem späteren Zeitpunkt wieder verwenden zu können.

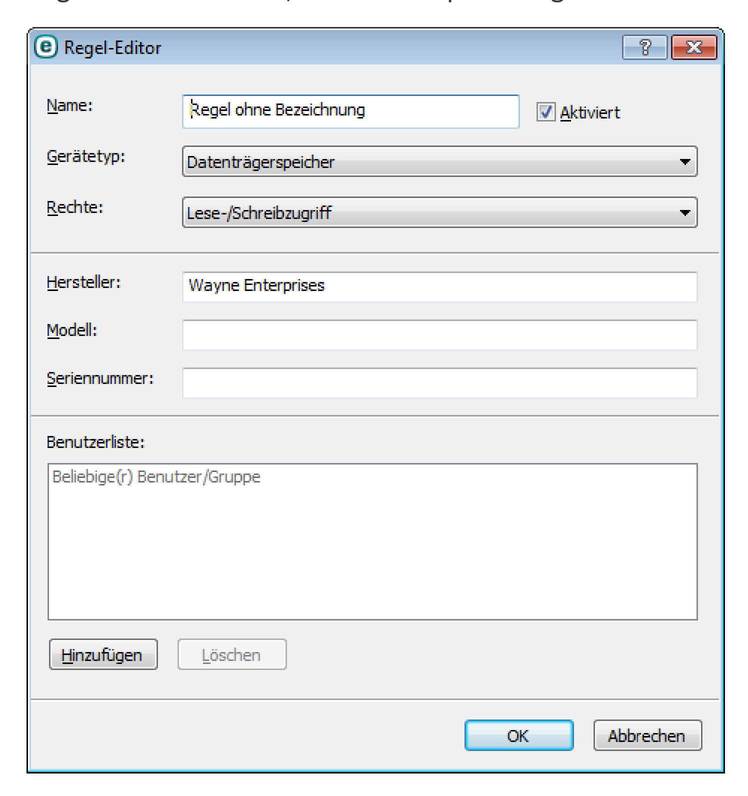
Die Regeln sind in nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden am Anfang der Liste angezeigt).

Mit einem Rechtsklick auf die Regel können Sie das Kontextmenü öffnen. Hier können Sie die in das Log zu schreibenden Mindestinformationen (Schweregrad) einer Regel festlegen. Um Log-Einträge anzuzeigen, klicken Sie im Hauptfenster von ESET Smart Security auf **Tools** > **Log-Dateien**.

Klicken Sie auf die Option **Auffüllen**, um automatisch die Parameter für am Computer angeschlossene Wechselmedien zu übernehmen.

4.1.3.2 Hinzufügen von Regeln für die Medienkontrolle

Eine Regel für die Medienkontrolle definiert die Aktion, die ausgeführt wird, wenn ein Gerät, das die Regelkriterien erfüllt, an den Computer angeschlossen wird.



Geben Sie zur leichteren Identifizierung der Regel im Feld **Name** eine Beschreibung ein. Über das Kontrollkästchen neben **Aktiviert** wird die Regel deaktiviert bzw. aktiviert. Dies ist beispielsweise nützlich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

Gerätetyp

Wählen Sie im Dropdown-Menü den Typ des externen Geräts aus (USB/Bluetooth/FireWire/...). Die Gerätetypen werden vom Betriebssystem übernommen und können im Geräte-Manager angezeigt werden, sofern ein Gerät an den Computer angeschlossen ist. Der Gerätetyp **Optischer Speicher** im Dropdown-Menü bezieht sich auf Datenspeicher auf optisch lesbaren Medien (z. B. CDs oder DVDs). Speichergeräte umfassen externe Datenträger oder herkömmliche Kartenlesegeräte, die über den USB- oder FireWire-Anschluss an den Computer angeschlossen sind. Smartcard-Lesegeräte umfassen Kartenlesegeräte für Smartcards mit eingebettetem integriertem Schaltkreis, beispielsweise SIM-Karten oder Authentifizierungskarten. Bildverarbeitungsgeräte sind beispielsweise Scanner oder Kameras. Diese Geräte liefern keine Informationen über Benutzer, sondern nur über deren Aktionen. Dies bedeutet, dass Bildverarbeitungsgeräte nur global gesperrt werden können.

Rechte

Der Zugriff auf andere Geräte als Speichergeräte kann entweder zugelassen oder gesperrt werden. Im Gegensatz dazu ist es für Speichergeräte möglich, eines der folgenden Rechte für die Regel auszuwählen:

- **Sperren** - Der Zugriff auf das Gerät wird gesperrt.
- **Nur Lesezugriff** - Nur Lesezugriff auf das Gerät wird zugelassen.
- **Lese-/Schreibzugriff** - Der vollständige Zugriff auf das Gerät wird zugelassen.

Beachten Sie, dass bestimmte Rechte (Aktionen) nur für bestimmte Gerätetypen verfügbar sind. Wenn das Gerät über Speicherplatz verfügt, sind alle drei Aktionen verfügbar. Bei anderen Geräten als Speichergeräten sind nur zwei Aktionen verfügbar. (Die Aktion **Nur Lesezugriff** ist für Bluetooth-Geräte nicht verfügbar. Diese Geräte können daher nur entweder gesperrt oder zugelassen werden).

Weitere Parameter zur Feinanpassung der Regeln und Anpassung an bestimmte Geräte. (die Groß-/Kleinschreibung muss nicht beachtet werden):

- **Hersteller** - Filtern nach Herstellername oder -ID.
- **Modell** - Die Bezeichnung des Geräts.
- **Seriennummer** - Externe Geräte verfügen üblicherweise über eigene Seriennummern. Bei CDs/DVDs bezieht sich die Seriennummer auf das Exemplar, nicht auf das Laufwerk.

Hinweis: Wenn die drei zuvor genannten Felder leer sind, ignoriert die Regel diese Felder bei der Zuordnung. Bei Filterparametern mit Textfeldern muss die Groß-/Kleinschreibung beachtet werden. Platzhalter (*, ?) werden nicht unterstützt. Die Werte müssen genau wie vom Hersteller festgelegt eingegeben werden.

Tipp: Um die Parameter eines bestimmten Geräts zu bestimmen, erstellen Sie eine Regel zum Zulassen des entsprechenden Gerätetyps, schließen Sie das Gerät an den Computer an und überprüfen Sie die Gerätedetails im Log für die Medienkontrolle.

Die Regeln können auf bestimmte Benutzer oder Benutzergruppen beschränkt werden, indem Sie diese zur **Benutzerliste** hinzufügen:

- **Hinzufügen** - Öffnet das Dialogfenster **Objekt Typ: Benutzer oder Gruppen**, in dem Sie bestimmte Benutzer auswählen können.
- **Entfernen** - Entfernt den ausgewählten Benutzer aus dem Filter.

Beachten Sie, dass nicht alle Geräte über Benutzerregeln eingeschränkt werden können (Bildverarbeitungsgeräte liefern z. B. keine Informationen über Benutzer, sondern nur über ausgeführte Aktionen).

4.1.4 HIPS

Das **Host Intrusion Prevention System** (HIPS) schützt Ihr System vor Schadsoftware und unerwünschten Programmaktivitäten, die negative Auswirkungen auf Ihren Computer haben könnten. HIPS analysiert das Verhalten von Programmen genau und nutzt Netzwerkfilter zur Überwachung von laufenden Prozessen, Dateien und Registrierungsschlüsseln. HIPS stellt eine zusätzliche Funktion zum Echtzeit-Dateischutz dar und ist keine Firewall, da nur die im Betriebssystem ausgeführten Prozesse überwacht werden.

Zugriff auf die HIPS-Einstellungen erhalten Sie über **Erweiterte Einstellungen** (F5). Klicken Sie in den erweiterten Einstellungen auf **Computer** > **HIPS**. Der Status von HIPS (aktiviert/deaktiviert) wird im Hauptfenster von ESET Smart Security angezeigt, im Bereich **Einstellungen** rechts vom Bereich „Computer“.

Warnung: Nur ein erfahrener Benutzer sollte die Einstellungen von HIPS ändern.

ESET Smart Security verfügt über eine integrierte *Self-Defense*-Technologie, die verhindert, dass Schadcode den Viren- und Spyware-Schutz beschädigt oder deaktiviert. *Self-Defense* schützt Dateien und Registrierungsschlüssel, die für die Funktionsfähigkeit von ESET Smart Security unabdingbar sind, und gewährleistet, dass potenzieller Schadcode nicht die erforderliche Berechtigung zum Ausführen von Änderungen an diesen Speicherorten erlangen kann.

Änderungen an den Optionen **HIPS aktivieren** und **Self-defense aktivieren** werden erst nach einem Neustart von Windows übernommen. Auch das Abschalten von **HIPS** erfordert einen Neustart des Computers.

Der **Exploit-Blocker** sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab. Weitere Informationen zu dieser Art des Schutzes finden Sie in unserem Glossar.

Die **Erweiterte Speicherprüfung** bietet im Zusammenspiel mit dem Exploit-Blocker stärkeren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung und/oder Verschlüsselung zu entgehen. Weitere Informationen zu dieser Art des Schutzes finden Sie in unserem Glossar.

Folgende vier Modi stehen für die HIPS-Filterung zur Verfügung:

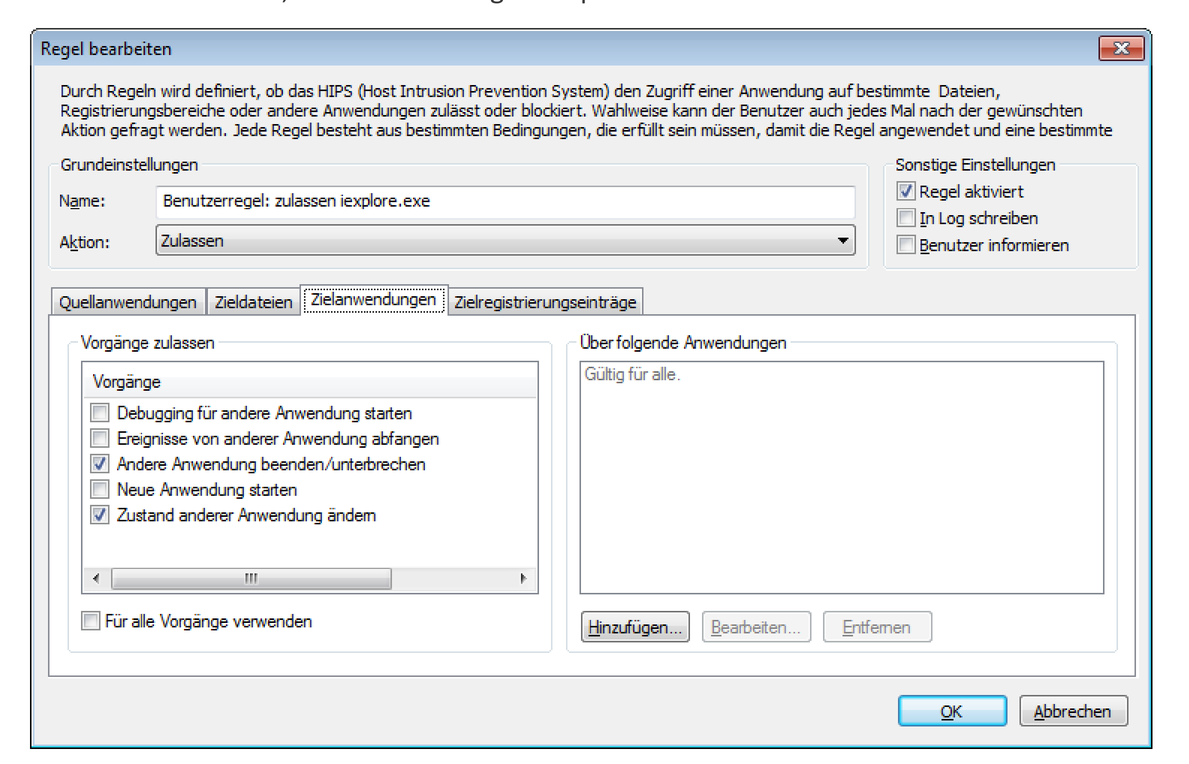
- **Automatischer Modus mit Regeln** - Vorgänge werden ausgeführt und vorab definierte Regeln zum Schutz Ihres Systems werden angewendet.
- **Interaktiver Modus** - Der Benutzer wird zur Bestätigung von Vorgängen aufgefordert.
- **Regelbasierter Filtermodus** - Vorgänge, die nicht in einer Regel definiert sind, können gesperrt werden.
- **Trainingsmodus** - Vorgänge werden ausgeführt, nach jedem Vorgang wird eine Regel erstellt. Die in diesem Modus erstellten Regeln können im **Regel-Editor** angezeigt werden, doch sie haben geringere Priorität als

manuell erstellte Regeln oder Regeln, die im automatischen Modus erstellt wurden. Wenn Sie die Option **Trainingsmodus** aktivieren, wird die Option **Benachrichtigung über Auslaufen des Trainingsmodus in X Tagen** wählbar. Nach Ablauf der in **Benachrichtigung über Auslaufen des Trainingsmodus in X Tagen** definierten Zeitspanne wird der Trainingsmodus wieder deaktiviert. Dieser Modus kann maximal 14 Tage andauern. Danach wird ein Fenster angezeigt, in dem Sie die Regeln bearbeiten und eine andere Filtermethode wählen können.

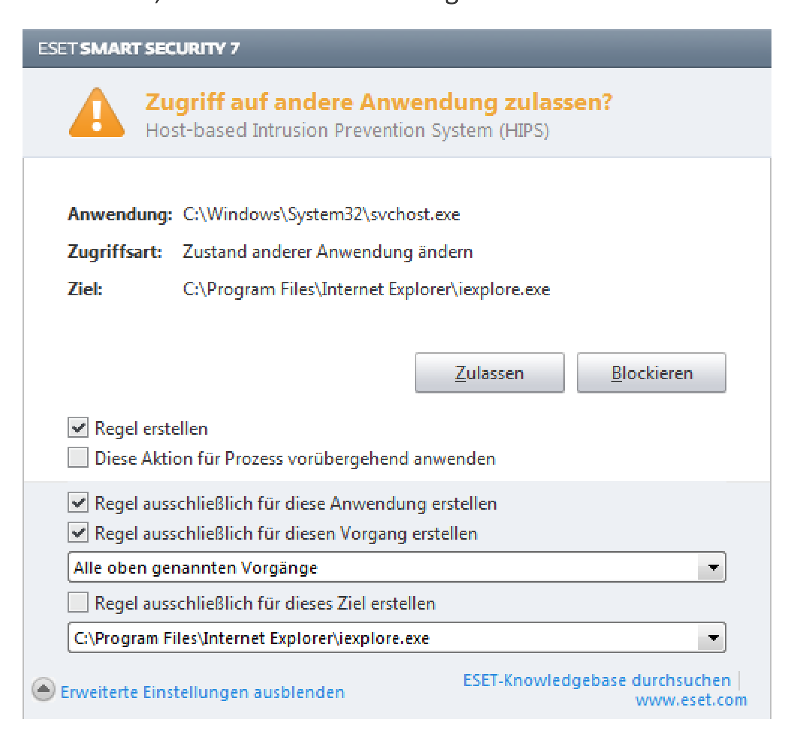
HIPS überwacht Ereignisse auf Betriebssystemebene und führt Aktionen gemäß Regeln aus, die den Regeln für die Personal Firewall in ESET Smart Security ähneln. Klicken Sie auf **Regeln konfigurieren...**, um das Fenster zur HIPS-Regelverwaltung zu öffnen. Hier können Sie Regeln auswählen, erstellen, bearbeiten und löschen.

Das folgende Beispiel zeigt, wie unerwünschtes Verhalten von Anwendungen beschränkt wird:

1. Benennen Sie die Regel und wählen Sie im Dropdown-Menü **Aktion** die Option **Sperren** aus.
2. Öffnen Sie die Registerkarte **Zielanwendungen**. Lassen Sie die Registerkarte **Quellanwendungen** leer, um die neue Regel auf alle Anwendungen anzuwenden, die einen der ausgewählten **Vorgänge** auf eine Anwendung aus der Liste **Über folgende Anwendungen** anzuwenden versuchen.
3. Wählen Sie die Option **Zustand anderer Anwendung ändern** (Sämtliche Vorgänge sind in der Produkthilfe beschrieben, die Sie über F1 aufrufen können.).
4. **Hinzufügen**: Fügen Sie eine oder mehrere Anwendungen hinzu, die Sie schützen möchten.
5. Aktivieren Sie das Kontrollkästchen **Benutzer informieren**, damit bei jedem Anwenden einer Regel ein Benachrichtigungsfenster angezeigt wird.
6. Klicken Sie auf **OK**, um die neue Regel zu speichern.



Wenn die Option **Fragen** als Standard ausgewählt ist, zeigt ESET Smart Security für jeden ausgeführten Vorgang ein Dialogfenster an. Dort können Sie den Vorgang entweder **Verweigern** oder **Zulassen**. Wenn Sie keine Aktion auswählen, wird eine Entscheidung anhand der vordefinierten Regeln getroffen.



Über das Dialogfenster **Zugriff auf andere Anwendung zulassen** können Sie eine Regel erstellen, die auf einer beliebigen neuen Aktion basiert, die HIPS erkennt, und dann die Bedingungen festlegen, unter denen die Aktion zugelassen oder verweigert werden soll. klicken Sie auf **Optionen anzeigen**, um die genauen Parameter für Ihre neue Regel zu definieren. Regeln, die auf diese Weise erstellt wurden, und manuell erstellte Regeln sind gleichrangig, daher können erstere allgemeiner sein als die Regel, die das Dialogfenster ausgelöst hat. Derselbe Vorgang kann also die Anzeige eines anderen Fensters auslösen, nachdem eine solche Regel erstellt wurde, wenn die Parameter Ihrer vorherigen Regeln nicht auf die Situation zutreffen.

Wenn Sie die Option Aktion für Prozess vorübergehend anwenden aktivieren, wird die Aktion (**Zulassen**/ **Blockieren**) bis zu einer Änderung der Regeln oder des Filtermodus, zum Update des HIPS-Moduls bzw. bis zum nächsten Systemstart angewendet. Nach einer dieser Aktionen werden die vorübergehenden Regeln gelöscht.

4.1.5 Gamer-Modus

Der Gamer-Modus ist eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Der Gamer-Modus kann auch während Präsentationen verwendet werden, die nicht durch eine Aktion des Virenschutzes unterbrochen werden dürfen. Ist dieser Modus aktiviert, so werden alle Popup-Fenster deaktiviert und die Aktivität des Taskplaners wird komplett gestoppt. Der Systemschutz läuft weiter im Hintergrund, doch es sind keine Eingaben durch Benutzer erforderlich.

Um den Gamer-Modus zu aktivieren, klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Computer** und dann unter **Gamer-Modus** auf **Aktivieren**. Alternativ können Sie den Gamer-Modus über die erweiterten Einstellungen (F5) aktivieren, indem Sie den Eintrag **Computer** erweitern, auf **Gamer-Modus** klicken und das Kontrollkästchen neben **Gamer-Modus aktivieren** aktivieren. Im Gamer-Modus besteht ein erhöhtes Risiko. Daher wird das Schutzstatus-Symbol in der Taskleiste orange und mit einer Warnung angezeigt. Diese Warnung wird auch im Hauptprogrammfenster angezeigt.

Wenn Sie die Option **Gamer-Modus automatisch aktivieren, wenn Anwendungen im Vollbildmodus ausgeführt werden** aktivieren, wird der Gamer-Modus gestartet, sobald Sie eine Anwendung im Vollbildmodus ausführen. Der Gamer-Modus wird beendet, sobald Sie die Anwendung beenden. Dies ist besonders hilfreich, um den Gamer-Modus direkt nach dem Start eines Computerspiels, einer Anwendung im Vollbildmodus oder einer Präsentation starten zu lassen.

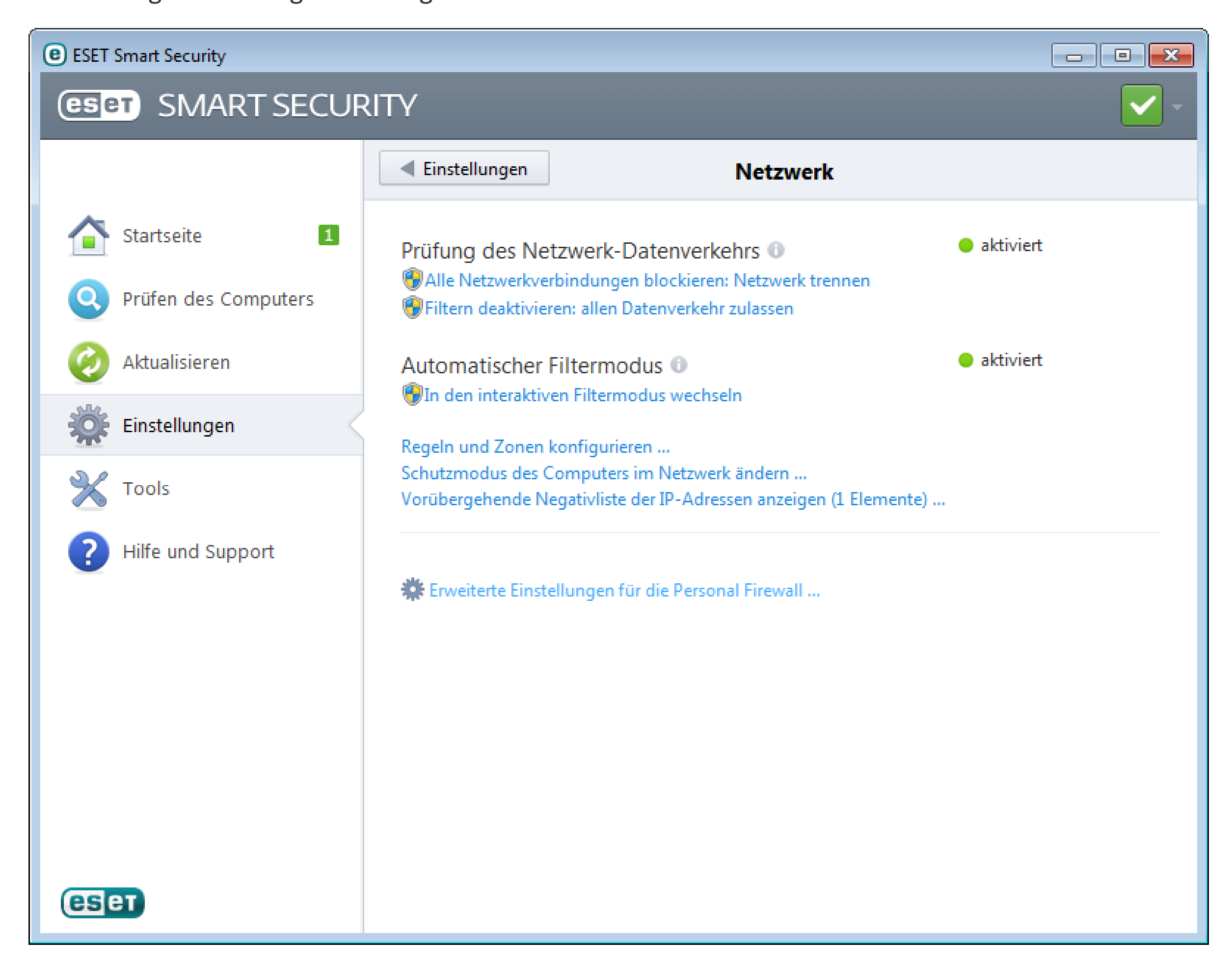
Sie können auch die Option **Gamer-Modus automatisch deaktivieren nach** aktivieren und eine Zeitspanne angeben (standardmäßig ist 1 Minute eingestellt), nach der der Gamer-Modus automatisch deaktiviert wird.

HINWEIS: Wenn für die Personal Firewall der interaktive Filtermodus eingestellt ist und der Gamer-Modus aktiviert sind, kann es zu Problemen beim Aufbau einer Internetverbindung kommen. Dies kann beim Ausführen eines Online-Spiels zu Problemen führen. Üblicherweise müssen Sie eine solche Aktion bestätigen (sofern keine Verbindungsregeln oder -ausnahmen festgelegt wurden), doch im Gamer-Modus kann der Benutzer keine derartigen Eingaben machen. Um dies zu umgehen, muss entweder eine Verbindungsregel für jede Anwendung festgelegt werden, mit der es im Gamer-Modus zu Konflikten kommen kann, oder es muss eine andere Filtermethode für die Personal Firewall gewählt werden. Bedenken Sie, dass Sie im Gamer-Modus bei dem Versuch, eine Website zu besuchen oder eine Anwendung auszuführen, die möglicherweise Sicherheitsrisiken darstellen, nicht benachrichtigt bzw. gewarnt werden, dass diese blockiert sind. Grund dafür ist die deaktivierte Benutzerinteraktion.

4.2 Netzwerk

Die Personal Firewall kontrolliert den gesamten Netzwerkdatenverkehr vom und zum System. Dabei werden einzelne Netzwerkverbindungen anhand zuvor festgelegter Filterregeln zugelassen oder blockiert. Die Firewall bietet Schutz gegen Angriffe von Remotecomputern und blockiert bestimmte Dienste. Sie bietet zudem auch Virenschutz für HTTP-, POP3- und IMAP-Protokolle. Mit diesen Funktionen ist die Personal Firewall ein wirksames Hilfsmittel zum Schutz Ihres Computers.

Sie können die Personal Firewall im Fenster **Einstellungen** unter **Netzwerk** konfigurieren. Dort können Sie den Filtermodus, Regeln und erweiterte Einstellungen anpassen. Dort können Sie außerdem auf erweiterte Einstellungen des Programms zugreifen.



Sämtlichen Netzwerkverkehr blockieren: Vom Netzwerk trennen klicken. Alle ein- und ausgehenden Verbindungen werden von der Personal Firewall blockiert. Verwenden Sie diese Option nur, wenn Sie schwerwiegende Sicherheitsrisiken befürchten, die eine Trennung der Netzwerkverbindung erfordern.

Filterung deaktivieren: allen Verkehr zulassen löst das Gegenteil der Blockierung des gesamten Netzwerkverkehrs aus. Wenn Sie diese Option auswählen, werden alle Filteroptionen der Personal Firewall deaktiviert und alle eingehenden und ausgehenden Verbindungen zugelassen. Dies hat die gleichen Auswirkungen, als wenn keine Firewall vorhanden wäre. Wenn die Prüfung des Netzwerk-Datenverkehrs **blockiert** ist, aktiviert die Option

Filtermodus aktivieren die Firewall.

Automatischer Filtermodus (wenn der automatische Filtermodus aktiviert ist) - Um den Filtermodus zu ändern, klicken Sie auf die Option **Interaktiven Filtermodus aktivieren**.

Interaktiver Filtermodus (wenn der interaktive Filtermodus aktiviert ist) - Um den Filtermodus zu ändern, klicken Sie auf die Option **Automatischen Filtermodus aktivieren (mit benutzerdefinierten Regeln)**.

Einstellungen für Zonen und Regeln - Öffnet das Einstellungsfenster für Zonen und Regeln, in dem Sie festlegen können, wie die Firewall mit Netzwerkverbindungen umgehen soll.

Schutzmodus Ihres Computers im Netzwerk ändern - Diese Einstellung bestimmt, wie zugänglich Ihr Computer für andere Computer im Netzwerk ist - wählen Sie zwischen maximalem und zugelassenem Schutzmodus.

Vorübergehende Negativliste für IP-Adressen anzeigen...- Zeigt eine Liste von IP-Adressen an, die als Angriffsquellen identifiziert und zur Negativliste hinzugefügt wurden, um die Verbindung für einen bestimmten Zeitraum zu unterbinden. Für weitere Informationen klicken Sie auf diese Option und drücken Sie die Taste F1.

Erweiterte Einstellungen für Personal Firewall... - Mit dieser Option haben Sie Zugriff auf die erweiterten Einstellungen für die Firewall.

4.2.1 Filtermodus

Für die ESET Smart Security Personal Firewall stehen fünf Filtermodi zur Verfügung. Diese finden Sie im Fenster **Erweiterte Einstellungen** (F5). Klicken Sie dazu auf **Netzwerk** > **Personal Firewall**. Das Verhalten der Firewall ist davon abhängig, welcher Modus ausgewählt wurde. Die Filtermodi beeinflussen auch den Umfang der erforderlichen Benutzereingaben.

Folgende vier Modi stehen für das Filtern zur Verfügung:

Automatischer Filtermodus - Standardmodus. Dieser Modus ist für Benutzer geeignet, die eine einfache und komfortable Verwendung der Firewall bevorzugen, bei der keine Regeln definiert werden müssen. Im automatischen Filtermodus werden alle ausgehenden Verbindungen des entsprechenden Systems zugelassen und alle neuen Verbindungen blockiert, die von der Netzwerkseite ausgehen.

Interaktiver Filtermodus - Ermöglicht eine benutzerdefinierte Konfiguration für die Personal Firewall. Bei jeder gefundenen Verbindung, für die noch keine Regel besteht, wird ein Dialogfenster angezeigt, in dem auf die unbekannte Verbindung hingewiesen wird. Der Benutzer kann entscheiden, ob die Verbindung zugelassen oder blockiert werden soll, und diese Auswahl kann als neue Regel für die Personal Firewall übernommen werden. Wenn eine neue Regel erstellt wurde, werden Verbindungen dieser Art beim nächsten Verbindungsversuch entsprechend der Regel automatisch zugelassen oder blockiert.

Regelbasierter Filtermodus - blockiert alle Verbindungen, für die keine Regel besteht, nach der diese zugelassen werden. Mit diesem Modus können erfahrene Benutzer Regeln festlegen, um nur erwünschte und sichere Verbindungen zuzulassen. Alle anderen Verbindungen werden von der Personal Firewall blockiert.

Trainingsmodus - Erstellt und speichert automatisch Regeln und eignet sich für die Ersteinrichtung der Personal Firewall. Es ist keine Benutzerinteraktion erforderlich, weil ESET Smart Security Regeln entsprechend der vordefinierten Parameter speichert. Der Trainingsmodus ist nicht sicher und sollte nur solange verwendet werden, bis alle Regeln für die erforderlichen Verbindungen erstellt wurden.

Profile sind ein Hilfsmittel, um das Verhalten der Personal Firewall von ESET Smart Security zu steuern.

4.2.1.1 Trainingsmodus

Im Trainingsmodus der Personal Firewall von ESET Smart Security wird für jede im System hergestellte Verbindung automatisch eine Regel erstellt und gespeichert. Es ist keine Benutzerinteraktion erforderlich, weil ESET Smart Security Regeln entsprechend der vordefinierten Parameter speichert.

Dieser Modus ist nicht sicher und wird nur für die Erstinstallation der Personal Firewall empfohlen.

Aktivieren Sie den Trainingsmodus unter **Einstellungen** > **Netzwerk** > **Personal Firewall** > **Trainingsmodus**, um die Optionen für den Trainingsmodus anzuzeigen. Dieser Bereich enthält die folgenden Elemente:

Warnung: Während sich die Personal Firewall im Trainingsmodus befindet, wird die Kommunikation nicht geprüft. Alle aus- und eingehenden Verbindungen werden zugelassen. In diesem Modus ist der Computer nicht vollständig durch die Personal Firewall geschützt.

Kommunikationsart - Wählen Sie die einzelnen Richtlinien zur Regelerstellung für jede Kommunikationsart aus. Es gibt vier Arten von Kommunikation:

- **Eingehender Datenverkehr aus der vertrauenswürdigen Zone** - Ein Beispiel für eine eingehende Verbindung innerhalb der vertrauenswürdigen Zone wäre ein Remotecomputer aus der vertrauenswürdigen Zone, der versucht, eine Verbindung zu einer Anwendung auf Ihrem Computer herzustellen.
- **Ausgehender Datenverkehr in die vertrauenswürdige Zone** - Eine lokale Anwendung versucht, eine Verbindung zu einem anderen Computer im lokalen Netzwerk oder innerhalb der vertrauenswürdigen Zone herzustellen.
- **Eingehender Datenverkehr aus dem Internet** - Ein Remotecomputer versucht, eine Verbindung zu einer Anwendung auf dem Computer herzustellen.
- **Ausgehender Datenverkehr in das Internet** - Eine lokale Anwendung versucht, eine Verbindung zu einem anderen Computer herzustellen.

Richtlinie zur Erstellung von Regeln - In diesem Bereich können Sie Parameter festlegen, die den neu erstellten Regeln hinzugefügt werden.

Lokalen Port hinzufügen - Die Nummer des lokalen Ports der Netzwerkkommunikation wird eingeschlossen. Bei ausgehenden Verbindungen werden normalerweise zufällige Nummern generiert. Daher wird empfohlen, diese Option nur für eingehende Verbindungen zu aktivieren.

Anwendung hinzufügen - Der Name der lokalen Anwendung wird eingeschlossen. Diese Option eignet sich für zukünftige Regeln auf Anwendungsebene (Regeln, die die Kommunikation für eine ganze Anwendung festlegen). Sie können beispielsweise nur die Kommunikation eines Webbrowsers oder E-Mail-Programms zulassen.

Remote-Port hinzufügen - Die Nummer des Remote-Ports der Netzwerkkommunikation wird eingeschlossen. Sie können beispielsweise einen bestimmten, mit einer Standardportnummer (HTTP - 80, POP3 - 110 usw.) verbundenen Dienst zulassen oder verweigern.

Remote-IP-Adresse / vertrauenswürdige Zone hinzufügen - Eine Remote-IP-Adresse oder Zone kann als Parameter für neue Regeln verwendet werden, die alle Netzwerkverbindungen zwischen dem lokalen System und diesen Remoteadressen/Zonen bestimmen. Diese Option eignet sich vor allem für die Definition von Aktionen eines bestimmten Computers oder einer Gruppe vernetzter Computer.

Höchstanzahl an unterschiedlichen Regeln für eine Anwendung - Wenn eine Anwendung über verschiedene Ports mit verschiedenen IP-Adressen usw. kommuniziert, erstellt der Trainingsmodus die richtige Anzahl Regeln für diese Anwendung. Diese Option ermöglicht Ihnen, die Anzahl der Regeln zu begrenzen, die für eine Anwendung erstellt werden können. Diese Option ist aktiv, wenn das Kontrollkästchen **Remote-Port hinzufügen** aktiviert wurde.

Benachrichtigung über Auslaufen des Trainingsmodus in X Tagen - Gibt die Anzahl der Tage an, nach denen ESET Smart Security den Benutzer darüber benachrichtigt, dass der Trainingsmodus noch aktiv ist. Diese Option soll den Benutzer davon abhalten, die Personal Firewall über einen längeren Zeitraum im Trainingsmodus zu betreiben. Nach Möglichkeit sollte die Personal Firewall nur kurzfristig in den Trainingsmodus versetzt werden, während die Benutzer die typischen Verbindungsarten initiieren. Im Trainingsmodus gespeicherte Netzwerkverbindungen

können als Grundlage für einen dauerhaft gültigen Satz Regeln verwendet werden.

4.2.2 Firewall-Profile

Mit Profilen können Sie das Verhalten der Personal Firewall von ESET Smart Security steuern. Beim Erstellen oder Bearbeiten einer Regel der Personal Firewall können Sie diese Regel einem bestimmten Profil zuordnen oder auf alle Profile anwenden. Wenn Sie ein Profil auswählen, werden nur die globalen Regeln (ohne Angabe eines Profils) sowie die Regeln angewendet, die diesem Profil zugeordnet wurden. Sie können mehrere Profile erstellen, denen unterschiedliche Regeln zugeordnet sind, um auf einfache Weise das Verhalten der Personal Firewall zu verändern.

Klicken Sie auf **Profile...** (siehe Abbildung im Abschnitt Filtermodus). Dort können Sie **Firewall-Profile** mit den Schaltflächen **Hinzufügen**, **Bearbeiten** oder **Entfernen** verwalten. Beachten Sie, dass ein Profil zum **Bearbeiten** oder **Entfernen** nicht im Dropdown-Menü **Ausgewähltes Profil** ausgewählt sein darf. Beim Hinzufügen oder Bearbeiten eines Profils können Sie auch die Bedingungen definieren, unter denen das Profil aktiviert wird.

Beim Erstellen eines Profils können Sie Ereignisse auswählen, die das Profil aktivieren. Folgende Optionen stehen zur Verfügung:

- **Nicht automatisch wechseln** - Die automatische Aktivierung ist ausgeschaltet (das Profil muss manuell aktiviert werden).
- **Wenn das automatische Profil ungültig und kein anderes Profil automatisch aktiviert wird (Standardprofil)** - Wenn das automatische Profil ungültig wird (d. h. Computer ist mit einem nicht vertrauenswürdigen Netzwerk verbunden - siehe Abschnitt Netzwerkauthentifizierung) und kein anderes an dessen Stelle aktiviert wird (Computer ist mit keinem anderen vertrauenswürdigen Netzwerk verbunden), wechselt die Personal Firewall zu diesem Profil. Nur ein einziges Profil kann diese Aktivierung verwenden.
- **Bei Authentifizierung dieser Zone** - Dieses Profil wird aktiviert, sobald die angegebene Zone authentifiziert ist (siehe Abschnitt Netzwerkauthentifizierung).

Wenn die Personal Firewall zu einem anderen Profil wechselt, wird in der rechten unteren Ecke neben der Systemuhr ein Hinweis angezeigt.

4.2.3 Konfigurieren und Verwenden von Regeln

Regeln fassen verschiedene Bedingungen zusammen, die eingesetzt werden, um alle Netzwerkverbindungen und damit verbundenen Aktionen wirksam zu prüfen. Mit den Regeln der Personal Firewall können Sie definieren, welche Aktion ausgeführt wird, wenn verschiedene Netzwerkverbindungen aufgebaut werden. Um auf die Filtereinstellungen für Regeln zuzugreifen, klicken Sie auf **Erweiterte Einstellungen** (F5) > **Netzwerk** > **Personal Firewall** > **Regeln und Zonen**.

Klicken Sie auf **Einstellungen...** im Abschnitt **Vertrauenswürdige Zone**, um das Dialogfenster „Einstellungen vertrauenswürdige Zone“ anzuzeigen. **Mit der Option Keinen Dialog mit Einstellungen vertrauenswürdiger Zonen anzeigen** können Sie festlegen, dass nicht jedes Mal, wenn ein neues Subnetz erkannt wird, auch das Fenster für die Einstellungen der vertrauenswürdigen Zone geöffnet wird. Es wird dann automatisch die aktuelle Zonenkonfiguration verwendet.

HINWEIS: Falls der **automatische Filtermodus** für die Personal Firewall ausgewählt wurde, sind manche Einstellungen nicht verfügbar.

Klicken Sie auf die Schaltfläche Einstellungen... im Abschnitt **Regel- und Zonen-Editor**, um das Fenster **Einstellungen für Zonen** anzuzeigen, in dem eine Übersicht von Regeln oder Zonen angezeigt wird (je nach aktiver Registerkarte). Das Fenster ist in zwei Abschnitte unterteilt. Im oberen Abschnitt sind alle Regeln in einer Kurzansicht aufgeführt. Im unteren Abschnitt werden Details zur ausgewählten Regel angezeigt. Unten im Fenster finden Sie die Schaltflächen **Neu**, **Bearbeiten** und **Löschen**, mit denen Einstellungen für Regeln vorgenommen werden können.

Es gibt zwei Arten von Verbindungen: eingehende und ausgehende. Eingehende Verbindungen gehen von einem Remotecomputer aus, der versucht, eine Verbindung mit dem lokalen System herzustellen. Ausgehende Verbindungen funktionieren in entgegengesetzter Richtung - die lokale Seite kontaktiert einen Remotecomputer.

Wenn eine neue, unbekannte Verbindung erkannt wird, sollten Sie genau prüfen, ob diese zugelassen oder

blockiert werden soll. Unerwünschte, unsichere oder unbekannte Verbindungen können ein Sicherheitsrisiko für Ihren Computer darstellen. Wenn eine solche Verbindung aufgebaut wird, sollten Sie besonders auf die Gegenstelle achten und prüfen, welche Anwendung versucht, mit ihrem Computer zu kommunizieren. Viele Schadprogramme versuchen, persönliche Daten zu erfassen und zu versenden oder weitere schädliche Anwendungen auf den Host-Computer zu laden. Mit Hilfe der Personal Firewall kann der Benutzer solche Verbindungen erkennen und beenden.

Über die Option **Daten zur Anwendung anzeigen** können Sie festlegen, wie Anwendungen in der Liste der Regeln angezeigt werden. Folgende Optionen stehen zur Verfügung:

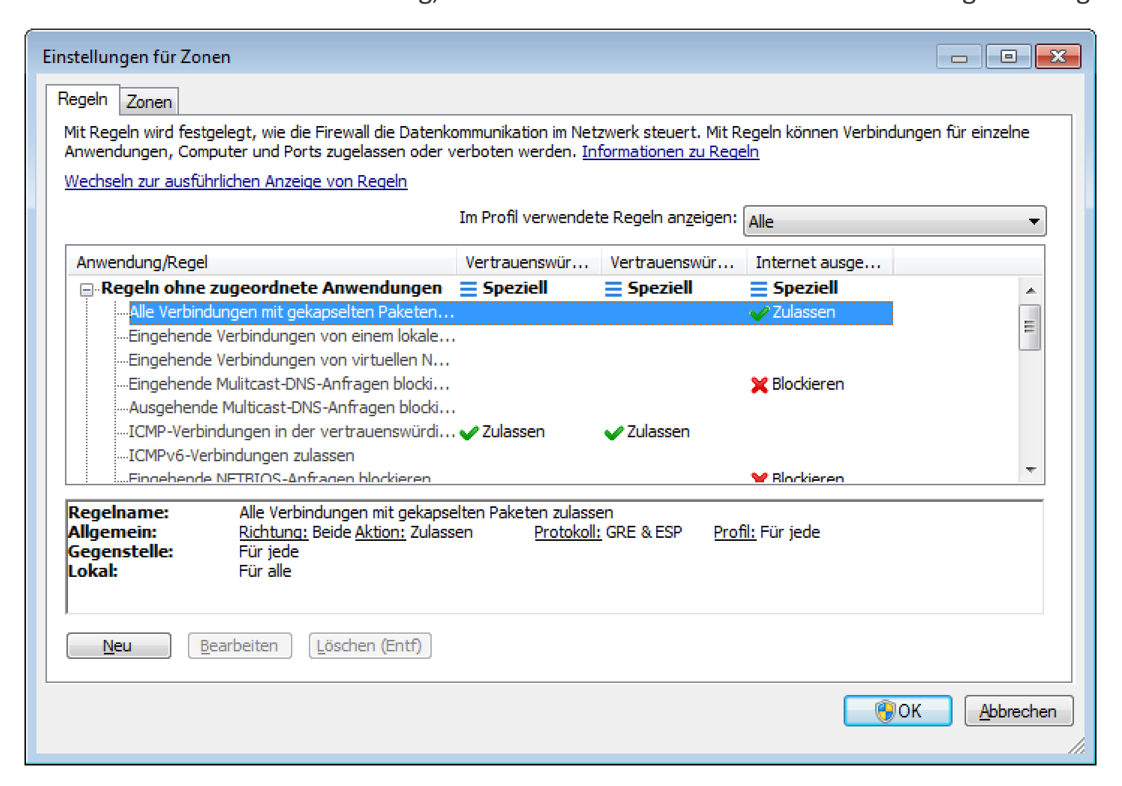
- **Vollständiger Pfad** - Vollständiger Pfad zur ausführbaren Programmdatei.
- **Beschreibung** - Beschreibung der Anwendung
- **Name** - Name der ausführbaren Programmdatei.

Legen Sie in der Liste **Anzuzeigende Regeln** fest, welche Regeltypen im Bereich Einstellungen für Regeln angezeigt werden sollen:

- **Nur benutzerdefinierte Regeln** - Nur die vom Benutzer erstellten Regeln werden angezeigt.
- **Benutzerdefinierte und vordefinierte Regeln** - Es werden alle benutzerdefinierten Regeln und die vordefinierten Standardregeln angezeigt.
- **Alle Regeln (auch System)** - Alle Regeln werden angezeigt.

4.2.3.1 Einstellungen für Regeln

Im Bereich „Einstellungen für Regeln“ werden alle Regeln angezeigt, die auf die Verbindungen einzelner Anwendungen mit vertrauenswürdigen Zonen und dem Internet angewendet werden. Regeln werden normalerweise automatisch erstellt, auf Basis der Reaktionen des Benutzers bei Verbindungsanfragen. Klicken Sie auf die Namen einer Anwendung, um weitere Informationen zur Anwendung anzuzeigen.



Vor den einzelnen Zeilen werden Plus-/Minuszeichen „+/-“ angezeigt. Klicken Sie auf diese Zeichen, um die Anzeige zu erweitern/zu reduzieren. Klicken Sie auf die Namen einzelner Anwendungen in der Spalte **Anwendung/Regel**, um Informationen zu den Anwendungen unten im Fenster anzuzeigen. Mit Hilfe des Kontextmenüs können Sie die Verbindungsanzeige anpassen. Außerdem können Sie mit Hilfe des Kontextmenüs Regeln hinzufügen, bearbeiten und löschen.

Vertrauenswürdige Zone ein-/ausgehend - Aktionen in Bezug auf ein- oder ausgehende Kommunikationen innerhalb der vertrauenswürdigen Zone.

Internet ein-/ausgehend - Aktionen in Bezug auf ein- oder ausgehende Internetverbindungen.

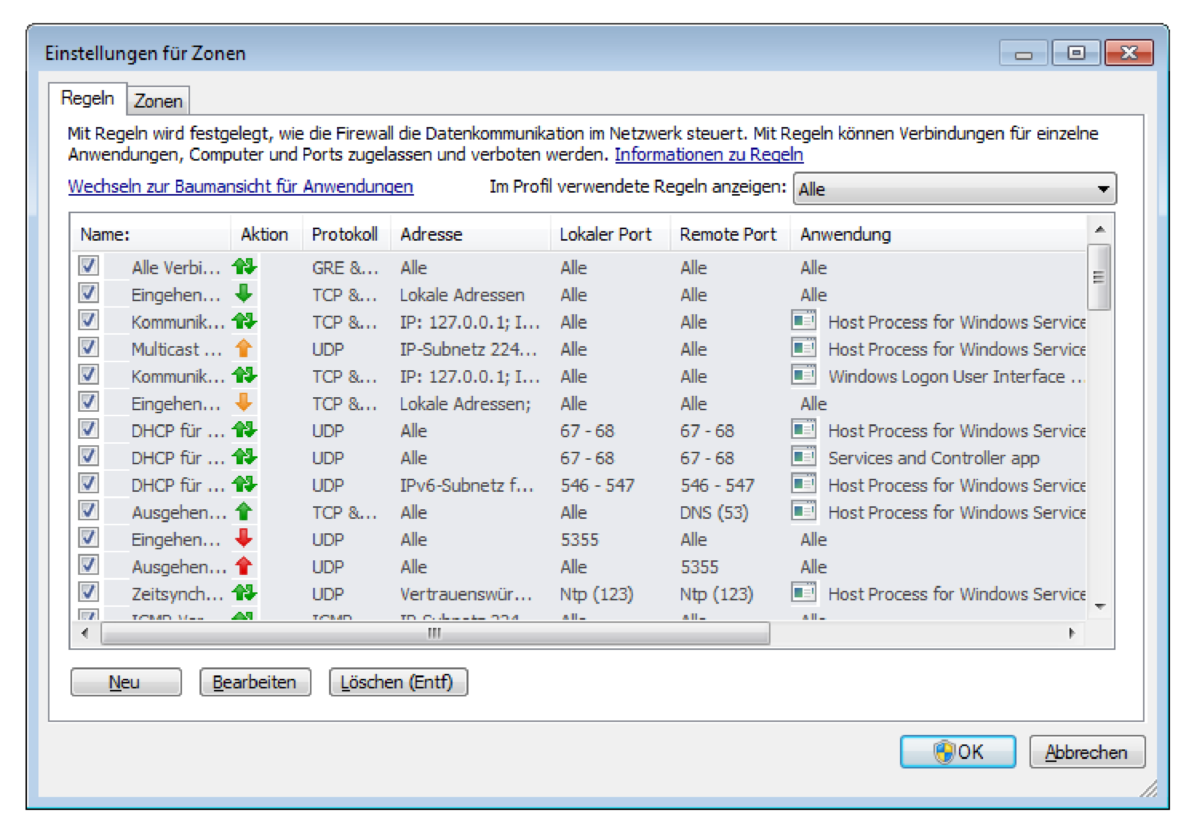
Für jeden Verbindungstyp und jede Verbindungsrichtung können Sie wählen:

- ✔ **Zulassen** - Verbindungen zulassen.
- ? **Fragen** - Sie werden bei jedem Verbindungsaufbau aufgefordert, die Verbindung zuzulassen oder zu blockieren.
- ✖ **Blockieren** - Verbindungen blockieren.
- ≡ **Speziell** - Keine Klassifizierung in Bezug auf die anderen Aktionen möglich. Wenn die Personal Firewall beispielsweise eine/n spezifische/n IP-Adresse oder Port zulässt, kann nicht mit Sicherheit gesagt werden, ob ein- oder ausgehender Datenverkehr für eine bestimmte Anwendung zulässig ist.

Wenn eine neue Anwendung installiert wird, die auf das Netzwerk zugreift, oder bei einer Veränderung an einer bestehenden Verbindung (Gegenstelle, Portnummer usw.) muss eine neue Regel erstellt werden. Um eine bestehende Regel zu bearbeiten, klicken Sie auf die Registerkarte **Regeln** und dann auf **Bearbeiten**.

4.2.3.1.1 Detaillierte Ansicht aller Regeln

Zur Anzeige der folgenden Daten im Fenster „Einstellungen für Zonen und Regeln“ klicken Sie auf **Wechseln zur ausführlichen Anzeige von Regeln**.



Name - Name der Regel. Zur Aktivierung der Regel muss das Kontrollkästchen aktiviert sein.

Aktion - Zeigt die Verbindungsrichtung und die Aktion an.

- Ausgehende Verbindungen sind zugelassen.
- Ausgehende Verbindungen werden blockiert.
- Eingehende Verbindungen sind zugelassen.
- Eingehende Verbindungen werden blockiert.
- Alle Verbindungen sind zugelassen.
- Bei allen Verbindungen wird ein Dialogfenster angezeigt, über das Sie eine Verbindung zulassen oder blockieren können.
- Alle Verbindungen werden blockiert.

Protokoll - Übertragungsprotokoll

Adresse - Adresse des Remotecomputers

Lokaler Port - Port des lokalen Computers

Remote Port - Port des Remote-Computers (Gegenstelle)

Awendung - Anwendung, auf die die Regel angewendet wird

Geändert - Datum der letzten Änderung

Profil - Wählen Sie aus dem Dropdown-Menü **Im Profil verwendete Regeln anzeigen** ein Profil aus, um die Regeln für das Profil anzuzeigen.

Erstellt/Geändert - Name des Benutzers, der die Regel geändert hat

Neu - Erstellen einer neuen Regel

Bearbeiten - Bearbeiten bestehender Regeln

Löschen (Entf) - Löschen bestehender Regeln

4.2.3.2 Regeln bearbeiten

Eine Änderung der Einstellungen ist immer dann erforderlich, wenn sich die überwachten Parameter geändert haben. In diesem Fall erfüllt die Regel nicht die Bedingungen und die festgelegte Aktion kann nicht ausgeführt werden. Wenn sich die Parameter geändert haben, wird die entsprechende Verbindung eventuell blockiert, wodurch Probleme bei der Ausführung der Anwendung entstehen können. Ein typisches Beispiel hierfür ist eine Änderung der Netzwerkadresse oder Portnummer der Gegenstelle.

Im oberen Teil des Fensters werden drei Registerkarten angezeigt:

- **Allgemein** - Geben Sie einen Regelnamen sowie die Verbindungsrichtung, die Aktion, das Protokoll und das Profil an, für das die Regel gelten soll.
- **Lokal** - Zeigt Informationen zur lokalen Seite der Verbindung an, darunter die Nummer des lokalen Ports oder Portbereichs und den Namen der kommunizierenden Anwendung.
- **Remote (Gegenstelle)** - Auf dieser Registerkarte werden Informationen zum Remoteport (Portbereich) angezeigt. Hier können Sie auch eine Liste mit Remote-IP-Adressen oder Zonen für eine Regel angeben.

Protokoll bezeichnet das Übertragungsprotokoll, das für die Regel verwendet wird. Klicken Sie auf **Protokoll auswählen**, um das Fenster Protokoll auswählen zu öffnen.

Standardmäßig sind alle Regeln **Für jedes** Profil aktiviert. Wählen Sie alternativ ein benutzerdefiniertes Firewall-Profil über die Schaltfläche**Profile**.

Wenn Sie auf **Log** klicken, wird die mit der Regel verbundene Aktivität in einem Log aufgezeichnet. Wenn die Option **Benutzer informieren** aktiviert ist, wird beim Anwenden der Regel ein entsprechender Hinweis angezeigt.

Unten auf jeder der drei Registerkarten befindet sich eine Zusammenfassung der Regel. Sie finden die gleichen Informationen, wenn Sie im Hauptfenster auf die Regel klicken (**Tools** > **Netzwerkverbindungen**; Rechtsklick auf die Regel und Aktivierung der Option **Details anzeigen** (siehe Abschnitt Netzwerkverbindungen)).

Beim Erstellen einer neuen Regel müssen Sie im Feld **Name** einen Namen für die Regel eingeben. Wählen Sie im Dropdown-Menü **Richtung** die Verbindungsrichtung aus, auf die die Regel angewendet werden soll. Wählen Sie über das Dropdown-Menü **Aktion** aus, welche Aktion ausgeführt werden soll, wenn eine Verbindung mit der Regel übereinstimmt.

Ein gutes Beispiel für eine neue Regel ist der Zugriff des Webbrowsers auf das Netzwerk. Dies wird folgendermaßen konfiguriert:

- Aktivieren Sie in der Registerkarte **Allgemein** ausgehende Verbindungen über TCP und UDP.
- Fügen Sie in der Registerkarte **Lokal** den Prozess hinzu, der Ihrer Browseranwendung entspricht (z. B. „iexplore.exe“ für Internet Explorer).
- Aktivieren Sie auf der Registerkarte **Remote (Gegenstelle)** nur Portnummer 80, wenn Sie Standard-Webbrowser-Aktivitäten zulassen möchten.

4.2.4 Konfigurieren von Zonen

Sie können im Fenster **Einstellungen für Zonen** den Zonennamen, die Beschreibung, die Liste der Netzwerkadressen und die Zonenauthentifizierung angeben (siehe auch Zonenauthentifizierung - Client-Konfiguration).

Zonen sind Gruppen von Netzwerkadressen, die eine logische Gruppe bilden. Jeder Adresse in einer Gruppe werden ähnliche Regeln zugewiesen, die zentral für die Gruppe festgelegt werden können. Ein Beispiel für eine solche Gruppe ist die **Vertrauenswürdige Zone**. Die vertrauenswürdige Zone ist eine Gruppe von Netzwerkadressen, die als vertrauenswürdig eingestuft wurden und die durch die Personal Firewall nicht blockiert werden.

Diese Zonen können durch Klicken auf die Schaltfläche **Bearbeiten** auf der Registerkarte **Zonen** im Fenster **Einstellungen für Zonen und Regeln** konfiguriert werden. Geben Sie einen **Namen** und eine **Beschreibung** für die Zone ein und fügen Sie über die Schaltfläche **IPv4-/IPv6-Adresse hinzufügen** eine Remote-IP-Adresse hinzu.

4.2.4.1 Netzwerkauthentifizierung

Wenn Sie mit einem mobilen Computer arbeiten, sollten Sie vor dem Herstellen einer Verbindung zu einem Netzwerk dessen Vertrauenswürdigkeit prüfen. Die vertrauenswürdige Zone wird durch die lokale IP-Adresse der Netzwerkkarte identifiziert. Mobile Computer melden sich oft an Netzwerken mit IP-Adressen an, die jenen der vertrauenswürdigen Netzwerke gleichen. Werden die Einstellungen für die vertrauenswürdige Zone nicht manuell auf **Netzwerk** gesetzt, verwendet die Personal Firewall weiterhin den Modus **Heim-/Firmennetzwerk**.

Um diese Situation zu vermeiden, empfehlen wir die Verwendung der Zonenauthentifizierung.

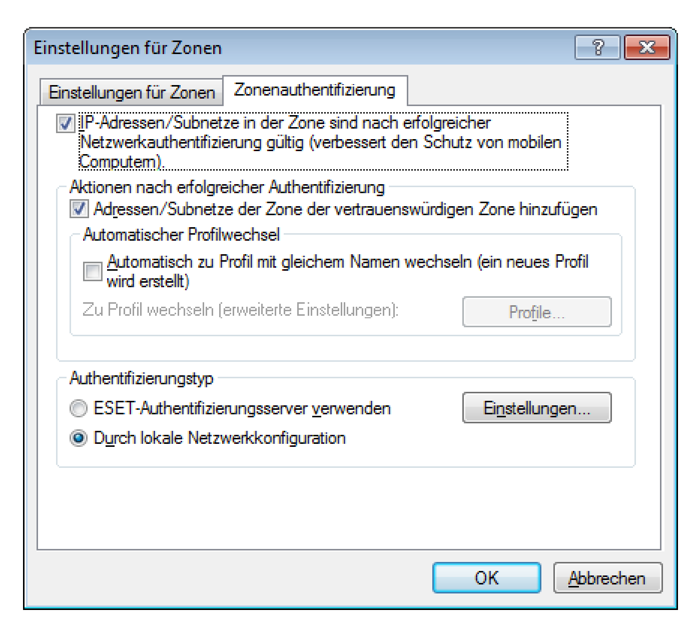
4.2.4.1.1 Zonenauthentifizierung - Client-Konfiguration

Klicken Sie im Fenster **Einstellungen für Zonen und Regeln** auf die Registerkarte **Zonen**, erstellen eine neue Zone, und verwenden Sie dabei den Namen der durch den Server authentifizierten Zone. Klicken Sie anschließend auf **IPv4-Adresse hinzufügen**, und wählen Sie die Option **Subnetz** aus, um eine Subnetzmaske hinzuzufügen, die den Authentifizierungsserver enthält.

Klicken Sie auf die Registerkarte **Zonenauthentifizierung**. Jede Zone kann für die Authentifizierung zum Server eingerichtet werden. Die Zone (ihre IP-Adresse und ihr Subnetz) sind gültig, nachdem sie erfolgreich authentifiziert wurde. Aktionen wie das Wechseln zu einem Firewall-Profil und Hinzufügen einer Adresse/eines Subnetzes der Zone zur vertrauenswürdigen Zone werden beispielsweise nur nach der erfolgreichen Authentifizierung durchgeführt.

Aktivieren Sie die Option **IP-Adressen/Subnetze in der Zone sind nach ... gültig** , damit die Zone ungültig wird, wenn die Authentifizierung nicht erfolgreich ist. Klicken Sie auf **Profile...**, um ein Personal Firewall-Profil auszuwählen, das nach erfolgreicher Zonenauthentifizierung aktiviert werden soll.

Wenn Sie die Option **Adressen/Subnetze der Zone der vertrauenswürdigen Zone hinzufügen** auswählen, werden die Adressen/Subnetze der Zone nach erfolgreicher Authentifizierung zur vertrauenswürdigen Zone hinzugefügt (empfohlen). Wenn die Authentifizierung nicht erfolgreich ist, werden die Adressen nicht zur vertrauenswürdigen Zone hinzugefügt. Wenn die Option **Automatisch zu Profil mit gleichem Namen wechseln (ein neues Profil wird erstellt)** aktiviert ist, wird nach erfolgreicher Authentifizierung ein neues Profil erstellt. Klicken Sie auf **Profile...**, um das Fenster Firewall-Profile zu öffnen.



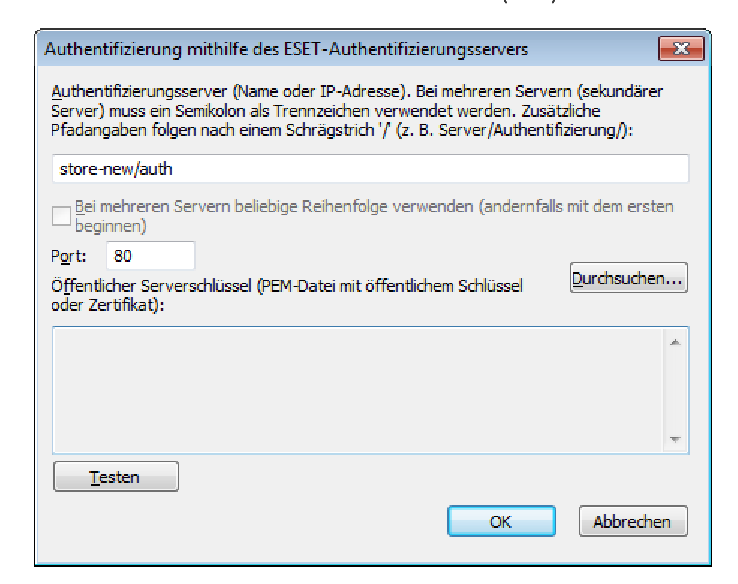
Für die Authentifizierung stehen zwei Verfahren zur Verfügung:

1. ESET-Authentifizierungsserver verwenden

Die Zonenauthentifizierung sucht nach einem bestimmten Server im Netzwerk und verwendet zur Serverauthentifizierung eine asymmetrische Verschlüsselung (RSA). Die Authentifizierung wird für jedes Netzwerk wiederholt, mit dem der Computer eine Verbindung erstellt. Klicken Sie auf **Einstellungen** und geben Sie einen Servernamen, einen Listening-Port für den Server und einen öffentlichen Serverschlüssel an, der dem privaten Serverschlüssel entspricht (siehe Abschnitt Zonenauthentifizierung - Server-Konfiguration). Der Servername kann in Form einer IP-Adresse, eines DNS oder eines NetBios-Namen angegeben werden. Der Servername kann von einem Pfad gefolgt sein, der den Speicherort des Schlüssels auf dem Server angibt (*z. B. Server_Name_/ Verzeichnis1/Verzeichnis2/Authentifizierung*). Geben Sie mehrere Server an (jeweils voneinander durch Semikolon getrennt), die als alternative Server agieren, falls der erste nicht verfügbar ist.

Der öffentliche Schlüssel kann eine Datei des folgenden Typs sein:

- PEM-verschlüsselter öffentlicher Schlüssel (.pem)
  Dieser Schlüssel kann mit dem ESET-Authentifizierungsserver generiert werden (siehe Abschnitt Zonenauthentifizierung - Serverkonfiguration).
- Verschlüsselter öffentlicher Schlüssel
- Zertifikat für öffentlichen Schlüssel (.crt)



Um die Einstellungen zu testen, klicken Sie auf **Testen**. Ist die Authentifizierung erfolgreich, wird der Hinweis *Serverauthentifizierung erfolgreich* angezeigt. Wenn die Authentifizierung nicht korrekt konfiguriert ist, wird eine der folgenden Fehlermeldungen angezeigt:

Fehler bei der Serverauthentifizierung. Die maximale Authentifizierungszeit ist abgelaufen.
Auf den Authentifizierungsserver kann nicht zugegriffen werden. Überprüfen Sie den Servernamen/die IP-Adresse, und/oder prüfen Sie die Einstellungen der Personal Firewall für die Bereiche Client und Server.

Fehler bei der Kommunikation mit dem Server.
Der Authentifizierungsserver wird nicht ausgeführt. Starten Sie den Authentifizierungsserver-Dienst (siehe Abschnitt Zonenauthentifizierung - Server-Konfiguration).

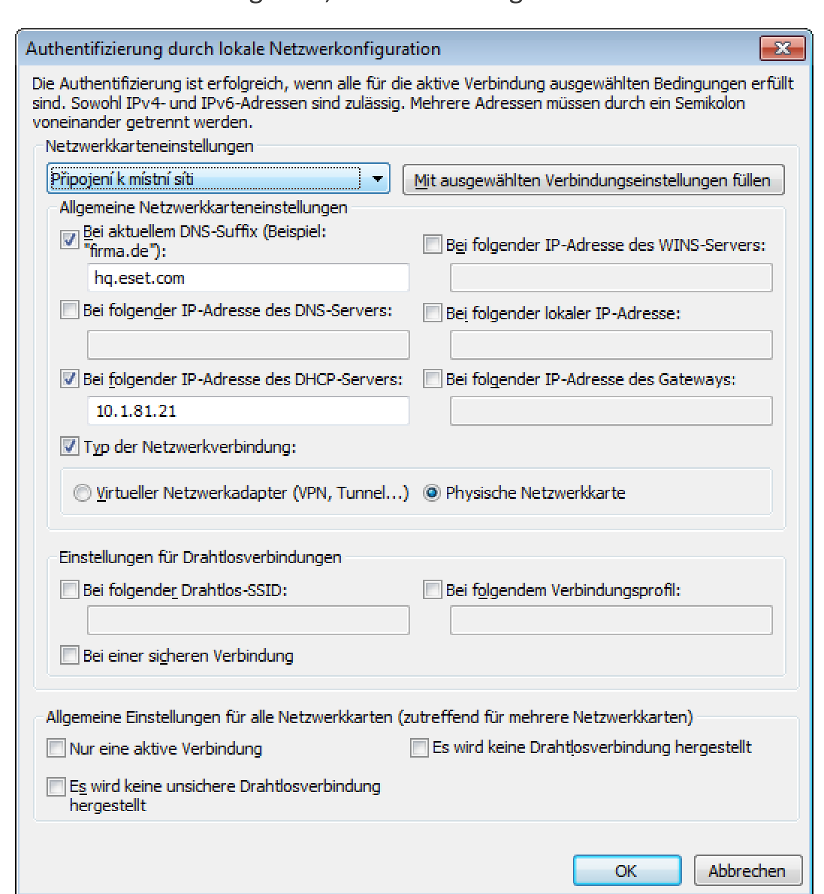
Der Name der Authentifizierungszone und die Serverzone stimmen nicht überein.
Der konfigurierte Zonenname entspricht nicht der Zone des Authentifizierungsservers. Überprüfen Sie beide Zonen, und stellen Sie sicher, dass ihre Namen identisch sind.

Fehler bei der Serverauthentifizierung. Serveradresse konnte in der Adressliste der angegebenen Zone nicht gefunden werden.
Die IP-Adresse des Computers, auf dem der Authentifizierungsserver ausgeführt wird, befindet sich außerhalb des in der aktuellen Zonenkonfiguration definierten IP-Adressbereichs.

Fehler bei der Serverauthentifizierung.. Es wurde möglicherweise ein ungültiger öffentlicher Schlüssel eingegeben.
Überprüfen Sie, ob der angegebene öffentliche Schlüssel dem privaten Serverschlüssel entspricht. Überprüfen Sie auch, ob die Datei des öffentlichen Schlüssels beschädigt ist.

2. Durch lokale Netzwerkkonfiguration

Die Authentifizierung erfolgt entsprechend den Parametern einer lokalen Netzwerkkarte. Die Authentifizierung einer Zone ist erfolgreich, wenn alle ausgewählten Parameter für die aktive Verbindung gültig sind.



4.2.4.1.2 Zonenauthentifizierung - Server-Konfiguration

Die Authentifizierung kann durch jeden Computer/Server ausgeführt werden, der mit dem zu authentifizierenden Netzwerk verbunden ist. Die Anwendung für den ESET-Authentifizierungsserver muss auf einem Computer/Server installiert sein, der jederzeit für die Authentifizierung verfügbar ist, wenn ein Client versucht, eine Verbindung mit dem Netzwerk herzustellen. Die Installationsdatei der Anwendung für den ESET-Authentifizierungsserver kann von der ESET-Website heruntergeladen werden.

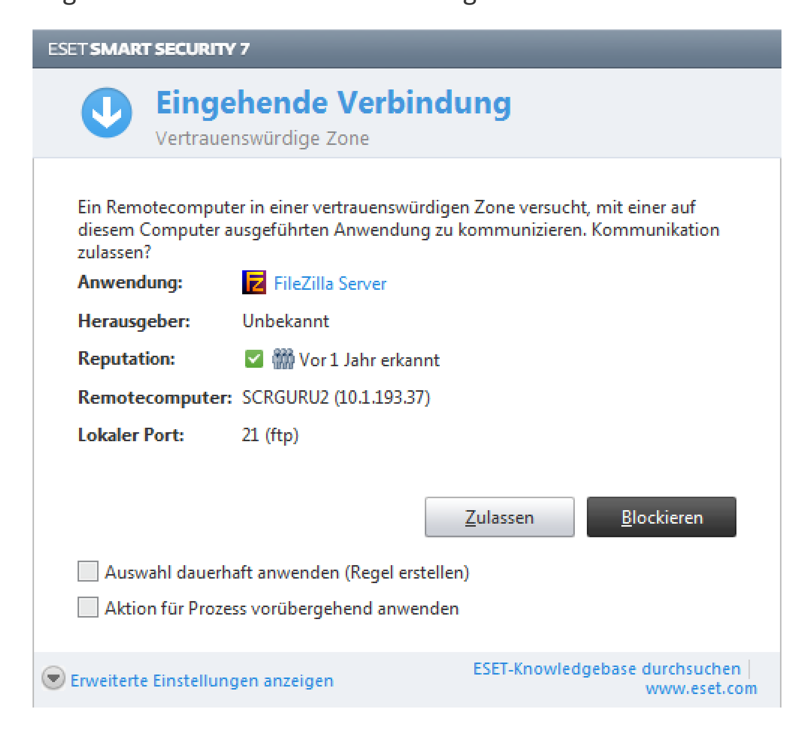
Nach der Installation der Anwendung für den ESET-Authentifizierungsserver wird ein Dialogfenster angezeigt (Sie können unter **Start** > **Alle Programme** > **ESET** > **ESET-Authentifizierungsserver** auf die Anwendung zugreifen).

Zum Konfigurieren des Authentifizierungsservers geben Sie den Namen der Authentifizierungszone, den Listening-Port für den Server (standardmäßig Port 80) und den Speicherort für den öffentlichen und den privaten Schlüssel ein. Erzeugen Sie dann den öffentlichen und den privaten Schlüssel, die bei der Authentifizierung verwendet werden. Der private Schlüssel verbleibt auf dem Server, während der öffentliche Schlüssel auf Seiten des Clients noch in die Authentifizierungszone importiert werden muss, die bei der Einrichtung der Firewall eingestellt wird.

4.2.5 Verbindung herstellen - Erkennung

Die Personal Firewall erkennt jede neu erstellte Netzwerkverbindung. Durch den aktivierten Firewall-Modus wird bestimmt, welche Vorgänge für die neue Regel ausgeführt werden. Wenn die Optionen **Automatischer Filtermodus** bzw. **Regelbasierter Filtermodus** aktiviert wurden, führt die Firewall die vordefinierten Aktionen automatisch aus.

Im interaktiven Filtermodus wird bei einer neu erkannten Netzwerkverbindung ein Fenster mit genauen Informationen angezeigt. Sie können dann entscheiden, ob die Verbindung zugelassen oder blockiert werden soll. Wenn dieselbe Verbindung im Dialogfenster mehrmals zugelassen wurde, sollte eine neue Regel erstellt werden. Wählen Sie dazu die Option **Auswahl dauerhaft anwenden (Regel erstellen)** und speichern Sie die Aktion als neue Regel für die Personal Firewall. Wenn die Firewall erneut dieselbe Verbindung erkennt, wird die entsprechende Regel ohne Benutzerinteraktion angewendet.



Seien Sie vorsichtig, wenn Sie neue Regeln erstellen. Lassen Sie nur bekannte, sichere Verbindungen zu. Wenn alle Verbindungen zugelassen werden, kann die Firewall ihren Zweck nicht erfüllen. Die wesentlichen Parameter für Verbindungen sind:

- **Gegenstelle** - Lassen Sie nur Verbindungen mit vertrauenswürdigen und bekannten Adressen zu.
- **Lokale Anwendung** - Es wird davon abgeraten, Verbindungen für unbekannte Anwendungen oder Prozesse zuzulassen.
- **Portnummer** - Verbindungen über übliche Ports (z. B. Web-Daten - Portnummer 80) können im Normalfall zugelassen werden.

Schadsoftware wird häufig über das Internet oder über versteckte Verbindungen verbreitet, um fremde Systeme zu infizieren. Wenn die Regeln richtig konfiguriert werden, ist die Personal Firewall ein wirksames Hilfsmittel zum Schutz vor verschiedensten Schadcode-Angriffen.

4.2.6 Erstellen von Logs

Die integrierte Personal Firewall von ESET Smart Security speichert alle wichtigen Vorgänge in einer Log-Datei, die direkt vom Hauptmenü aus aufgerufen werden kann. Klicken Sie auf **Tools** > **Log-Dateien** und wählen Sie **Personal Firewall** aus dem Dropdown-Menü **Log** aus.

Anhand der Log-Dateien können Sie Fehler und Eindringungsversuche in Ihr System erkennen. Die Log-Dateien der ESET Personal Firewall enthalten folgende Informationen:

- Datum und Uhrzeit des Ereignisses
- Name des Ereignisses
- Quelle
- Zieladresse
- Netzwerk-Übertragungsprotokoll
- Zugewiesene Regel oder, falls identifiziert, Name des Wurms
- Beteiligte Anwendung
- Benutzer

Eine gründliche Analyse dieser Daten kann wesentlich dazu beitragen, Angriffe auf die Systemsicherheit frühzeitig zu erkennen. Viele andere Faktoren können auf Sicherheitsrisiken hinweisen und sollten beobachtet werden, um mögliche Auswirkungen zu minimieren: häufige Verbindungen von unbekannten Standorten, ungewöhnlich viele Verbindungsversuche, Verbindungen mit unbekannten Anwendungen, Benutzung ungewöhnlicher Portnummern.

4.2.7 Systemintegration

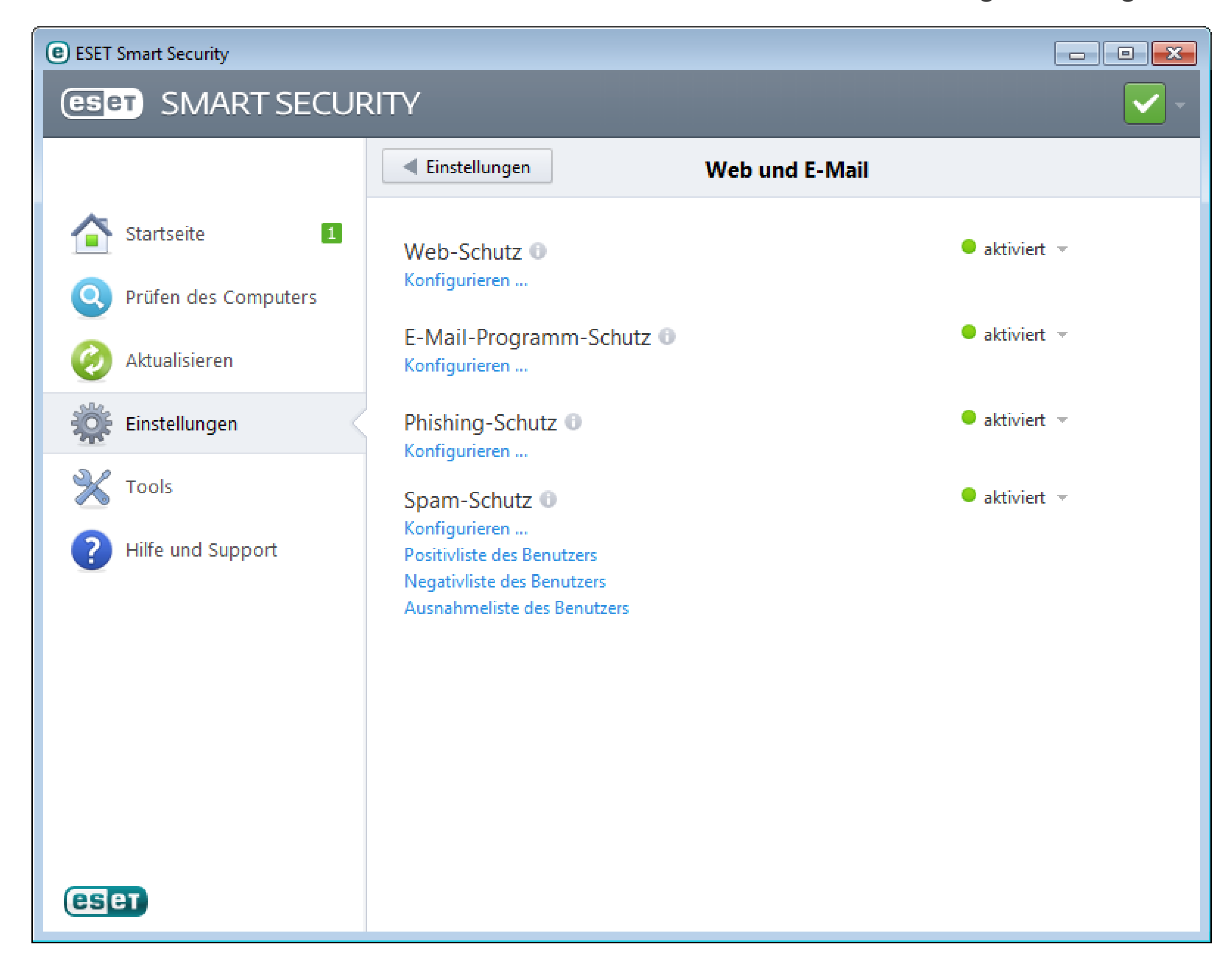
Die ESET Smart Security Personal Firewall kann auf mehreren Ebenen ausgeführt werden:

- **Alle Optionen sind aktiv** - Die Personal Firewall ist vollständig integriert und ihre Komponenten sind aktiv (Standardeinstellung). Wenn Ihr Computer mit einem großen Netzwerk oder dem Internet verbunden ist, sollten Sie diese Option aktiviert lassen. Dies ist die sicherste Einstellung der Personal Firewall, die einen hohen Schutz bietet.
- **Personal Firewall ist deaktiviert** - Die Personal Firewall ist in das System integriert und vermittelt die Netzwerkkommunikation, führt jedoch keine Überprüfungen auf Bedrohungen durch.
- **Nur anwendungsspezifische Protokolle prüfen** - Es sind nur diejenigen Komponenten der Personal Firewall aktiv, die anwendungsspezifische Protokolle (HTTP, POP3, IMAP und deren abgesicherte Versionen) prüfen. Wenn die anwendungsspezifischen Protokolle nicht geprüft werden, wird Ihr System mit dem Echtzeit-Dateischutz und der On-Demand-Prüfung überwacht.
- **Personal Firewall vollständig deaktiviert** - Aktivieren Sie diese Option, um die Personal Firewall vollständig zu deaktivieren. Es werden keine Prüfungen durchgeführt. Dies kann beim Ausführen von Tests nützlich sein: Wenn eine Anwendung gesperrt wird, können Sie überprüfen, ob die Sperre von der Firewall ausgeht. Diese Option bietet den geringsten Schutz und deaktiviert die Firewall vollständig. Verwenden Sie diese Option mit Vorsicht.

Update der Personal Firewall erst nach Neustart des Computers durchführen - Die Updates der Personal Firewall werden erst beim nächsten Neustart des Computers heruntergeladen und installiert.

4.3 Web und E-Mail

Sie können die Einstellungen für den Web- und E-Mail-Schutz im Fenster **Einstellungen** konfigurieren, indem Sie auf **Web und E-Mail** klicken. Von hier aus können Sie auf erweiterte Einstellungen des Programms zugreifen.



Der Internetzugang ist eine Standardfunktion von Computern. Leider ist das Internet mittlerweile auch der wichtigste Weg zur Verbreitung von Schadsoftware. Daher müssen Sie die Einstellungen des **Web-Schutzes** sorgfältig auswählen.

Klicken Sie auf **Konfigurieren**, um die Web-/E-Mail-/Phishing-/Spam- Schutzeinstellungen in den erweiterten Einstellungen zu öffnen.

Der E-Mail-Client-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3- und dem IMAP-Protokoll übertragen werden. Mithilfe der Plug-In-Software für Ihr E-Mail-Programm stellt ESET Smart Security Kontrollfunktionen für die gesamte ein- und ausgehende E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) bereit.

Der Phishing-Schutz blockiert Webseiten, die bekanntermaßen Phishing-Inhalte verbreiten. Es wird dringend empfohlen, den Phishing-Schutz aktiviert zu lassen.

Der **Spam-Schutz** filtert unerwünschte E-Mails heraus.

- **Positivliste des Benutzers** - Es wird ein Dialogfenster geöffnet, über das als sicher eingestufte E-Mail-Adressen hinzugefügt, bearbeitet oder gelöscht werden können. E-Mails, deren Absender in der Positivliste stehen, werden nicht auf Spam geprüft.
- **Negativliste des Benutzers** - Es wird ein Dialogfenster geöffnet, über das als unsicher eingestufte E-Mail-Adressen hinzugefügt, bearbeitet oder gelöscht werden können. E-Mails, deren Absender in der Negativliste stehen, werden als Spam eingestuft.
- **Ausnahmeliste des Benutzers** - Es wird ein Dialogfenster geöffnet, über das E-Mail-Adressen hinzugefügt, bearbeitet oder gelöscht werden können, die möglicherweise gefälscht wurden und als Spam-Absender verwendet werden. E-Mails, deren Absender in der Ausnahmeliste stehen, werden immer auf Spam geprüft. Standardmäßig enthält die Ausnahmeliste alle E-Mail-Adressen aus bestehenden E-Mail-Konten.

Sie können den Web-/E-Mail-/Phishing-Schutz deaktivieren/Spam- Schutzmodul kann durch Klicken auf **Aktiviert** vorübergehend deaktiviert werden.

4.3.1 E-Mail-Client-Schutz

Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3-Protokoll übertragen werden. Mithilfe der Plug-In-Software für Microsoft Outlook und andere E-Mail-Programme stellt ESET Smart Security Kontrollfunktionen für die gesamte E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) bereit. Für die Prüfung eingehender Nachrichten verwendet das Programm alle erweiterten ThreatSense-Prüfmethoden. Die Erkennung von Schadcode findet also noch vor dem Abgleich mit der Signaturdatenbank statt. Die Prüfung der POP3-Kommunikation erfolgt unabhängig vom verwendeten E-Mail-Programm.

Die Optionen für diese Funktion finden Sie unter **Erweiterte Einstellungen** > **Web und E-Mail** > **E-Mail-Client-Schutz**.

Einstellungen für ThreatSense - In diesem Bereich finden Sie erweiterte Einstellungen für den Virenschutz. Hier können Sie Einstellungen für zu prüfende Objekte, Erkennungsmethoden usw. festlegen. Klicken Sie auf **Einstellungen**, um die erweiterten Einstellungen für den Virenschutz anzuzeigen.

Nach erfolgter Prüfung kann ein Prüfhinweis zu der E-Mail-Nachricht hinzugefügt werden. Sie haben folgende Optionen: **Prüfhinweis zu eingehenden/gelesenen E-Mails hinzufügen** und **Prüfhinweis zu ausgehenden E-Mails hinzufügen**. Es kann jedoch nicht ausgeschlossen werden, dass bestimmte Bedrohungen Prüfhinweise in problematischen HTML-Nachrichten fälschen oder löschen. Prüfhinweise können zu empfangenen und gelesenen E-Mails und/oder zu gesendeten E-Mails hinzugefügt werden. Folgende Optionen stehen zur Verfügung:

- **Nie** - Es werden keine Prüfhinweise zu E-Mails hinzugefügt.
- **Nur an infizierte E-Mails** - Prüfhinweise werden nur E-Mails hinzugefügt, in denen Schadcode erkannt wurde (Standardeinstellung).
- **Bei allen geprüften E-Mails** - Alle geprüften E-Mails werden mit Prüfhinweisen versehen.

Prüfhinweis an den Betreff empfangener und gelesener/ausgehender infizierter E-Mails anhängen - Aktivieren Sie dieses Kontrollkästchen, wenn Prüfhinweise zu den Betreffzeilen infizierter E-Mails hinzugefügt werden sollen. Ohne großen Aufwand können Sie in Ihrem E-Mail-Programm eine Filterregel erstellen, die diesen Prüfhinweis erkennt (falls Ihr E-Mail-Programm Filterregeln unterstützt). Diese Funktion erhöht beim Empfänger auch die Glaubwürdigkeit von Nachrichten. Bei der Erkennung von eingedrungener Schadsoftware stehen wertvolle Informationen zur Verfügung, um den Bedrohungsgrad durch die Nachricht oder den Absender einzuschätzen.

Text, der zur Betreffzeile infizierter E-Mails hinzugefügt wird - Geben Sie hier den Text ein, der das Präfix in der Betreffzeile einer infizierten E-Mail ersetzen soll. Mit dieser Funktion wird der Nachrichtenbetreff *„Hallo“* mit dem voreingestellten Präfix *„[virus]“* folgendermaßen gekoppelt: *„[virus] Hallo“*. Dabei repräsentiert die Variable *% VIRUSNAME%* die erkannte Bedrohung.

4.3.1.1 Integration mit E-Mail-Programmen

Die Integration von ESET Smart Security mit E-Mail-Programmen verbessert den aktiven Schutz gegen Schadcode in E-Mail-Nachrichten. Wenn Ihr E-Mail-Programm dies unterstützt, kann die Integration in ESET Smart Security aktiviert werden. Bei aktivierter Integration wird die ESET Smart Security-Symbolleiste vom E-Mail-Programm übernommen, d. h. die Verbindungen werden kontrolliert und die E-Mail-Kommunikation wird dadurch sicherer. Die Integrationseinstellungen finden Sie unter **Einstellungen** > **Erweiterte Einstellungen...** > **Web und E-Mail** > **E-Mail-Client-Schutz** > **Integration in E-Mail-Programme**.

Zu den derzeit unterstützten E-Mail-Programmen gehören Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail und Mozilla Thunderbird (bis Version 5). Eine vollständige Liste der unterstützten E-Mail-Programme und Versionen finden Sie im entsprechenden ESET-Knowledgebase-Artikel.

Wählen Sie die Option **Prüfen neuer Elemente im Posteingang deaktivieren**, falls Sie während der Arbeit mit Ihrem E-Mail-Programm eine Systemverlangsamung bemerken. Dies kann der Fall sein, wenn Sie E-Mails vom Kerio Outlook Connector Store abrufen.

Auch bei nicht aktivierter Integration ist die E-Mail-Kommunikation durch den E-Mail-Client-Schutz (POP3, IMAP) weiterhin geschützt.

4.3.1.1.1 Konfiguration des E-Mail-Schutzes

Der E-Mail-Schutz unterstützt folgende E-Mail-Clients: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail und Mozilla Thunderbird (bis Version 5). Der E-Mail-Schutz ist ein Plug-In für diese Programme. Das Plugin funktioniert unabhängig vom eingesetzten Protokoll. Wenn beim E-Mail-Client eine verschlüsselte Nachricht eingeht, wird diese entschlüsselt und an das Virenschutz-Prüfmodul weitergeleitet.

Folgende E-Mails prüfen

Eingehende E-Mails - Aktiviert/deaktiviert die Überprüfung empfangener Nachrichten.
Ausgehende E-Mails - Aktiviert/deaktiviert die Überprüfung ausgehender Nachrichten.
E-Mails, die zum Lesen geöffnet werden - Aktiviert/deaktiviert die Überprüfung gelesener Nachrichten.

Aktion für infizierte E-Mails

Keine Aktion - Infizierte Anhänge werden erkannt, aber es werden keine Aktionen für E-Mails durchgeführt.
E-Mail löschen - Es werden Hinweise zu Bedrohungen angezeigt. Betroffene E-Mails werden gelöscht.
In den Ordner „Gelöschte Objekte“ verschieben - Infizierte E-Mails werden automatisch in den Ordner **Gelöschte Objekte** verschoben.
In folgenden Ordner verschieben - Geben Sie einen Ordner an, in den infizierte E-Mails nach der Erkennung verschoben werden sollen.

Sonstige

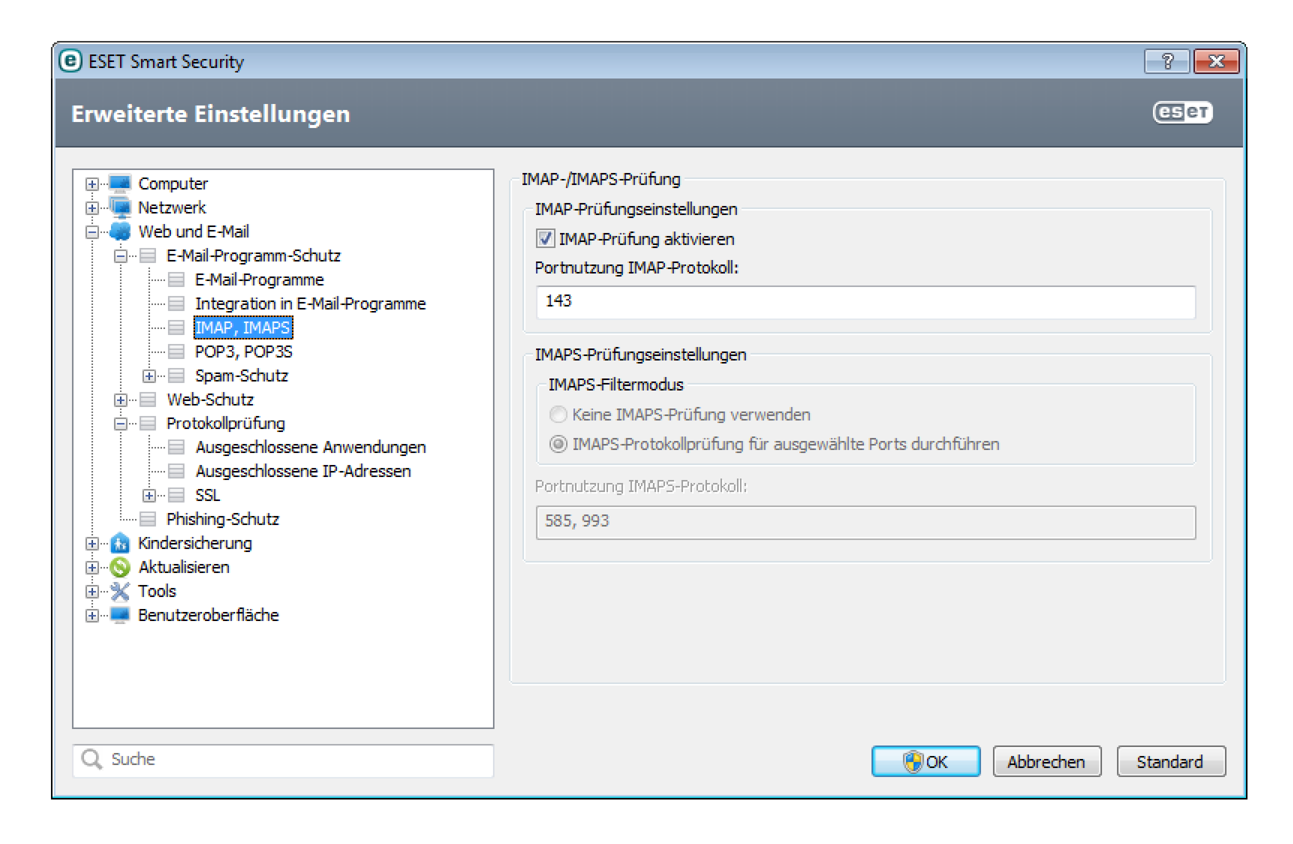
Nach Signaturdatenbank-Update E-Mails erneut prüfen - Aktiviert/deaktiviert die erneute Prüfung nach einem Signaturdatenbank-Update.
Prüfergebnisse von anderen Modulen entgegennehmen - Wenn diese Option aktiviert ist, nimmt das E-Mail-Schutz-Modul Prüfergebnisse von anderen Modulen entgegen.

4.3.1.2 IMAP-/IMAPS-Prüfung

IMAP (Internet Message Access Protocol) ist ein weiteres Internetprotokoll für das Abrufen von E-Mails. IMAP bietet gegenüber POP3 einige Vorteile. Beispielsweise können sich mehrere Clients gleichzeitig beim selben Postfach anmelden und Statusinformationen zu den Nachrichten pflegen, z. B. ob die Nachricht gelesen, beantwortet oder gelöscht wurde. ESET Smart Security schützt dieses Protokoll unabhängig vom eingesetzten E-Mail-Programm.

Das Modul, das diese Kontrollfunktion bereitstellt, wird automatisch beim Systemstart initialisiert und ist dann im Speicher aktiv. Die IMAP-Protokollprüfung wird automatisch ausgeführt, ohne dass das E-Mail-Programm neu konfiguriert werden muss. In der Standardeinstellung wird die gesamte Kommunikation über Port 143 geprüft. Bei Bedarf können weitere Kommunikationsports hinzugefügt werden. Mehrfache Portnummern müssen durch ein Komma voneinander getrennt sein.

Der Datenverkehr über verschlüsselte Verbindungen wird nicht geprüft. Zur Aktivierung der Prüfung verschlüsselter Verbindungen und zur Anzeige der Prüfeinstellungen navigieren Sie zu SSL-Protokollprüfung in den erweiterten Einstellungen, klicken Sie auf **Web und E-Mail** > **Prüfen von Anwendungsprotokollen** > **SSL** und aktivieren Sie die Option **SSL-Protokoll immer prüfen**.



4.3.1.3 POP3-, POP3S-Prüfung

Das POP3-Protokoll ist das am häufigsten verwendete Protokoll zum Empfangen von E-Mails mit einem E-Mail-Programm. ESET Smart Security bietet POP3-Protokoll-Schutzfunktionen unabhängig vom verwendeten E-Mail-Programm.

Das Modul, das diese Kontrollfunktion bereitstellt, wird automatisch beim Systemstart initialisiert und ist dann im Speicher aktiv. Um das Modul einsetzen zu können, muss es aktiviert sein. Die POP3-Prüfung wird automatisch ausgeführt, ohne dass das E-Mail-Programm neu konfiguriert werden muss. In der Standardeinstellung wird die gesamte Kommunikation über Port 110 geprüft. Bei Bedarf können weitere Kommunikationsports hinzugefügt werden. Mehrfache Portnummern müssen durch ein Komma voneinander getrennt sein.

Der Datenverkehr über verschlüsselte Verbindungen wird nicht geprüft. Zur Aktivierung der Prüfung verschlüsselter Verbindungen und zur Anzeige der Prüfeinstellungen navigieren Sie zu SSL-Protokollprüfung in den erweiterten Einstellungen, klicken Sie auf **Web und E-Mail** > **Prüfen von Anwendungsprotokollen** > **SSL** und aktivieren Sie die Option **SSL-Protokoll immer prüfen**.

In diesem Abschnitt können Sie die Prüfung der Protokolle POP3 und POP3S konfigurieren.

Prüfen von E-Mails aktivieren - Wenn diese Option aktiviert ist, werden alle Daten geprüft, die über POP3 übertragen werden.

Portnutzung POP3-Protokoll - Eine Liste von Ports, die vom POP3-Protokoll verwendet werden (standardmäßig 110).

ESET Smart Security unterstützt auch die Überwachung von POP3S-Protokollen. Bei dieser Kommunikationsart wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET Smart Security überwacht die mit Hilfe der Verschlüsselungsverfahren SSL (Secure Socket Layer) und TLS (Transport Layer Security) abgewickelte Kommunikation.

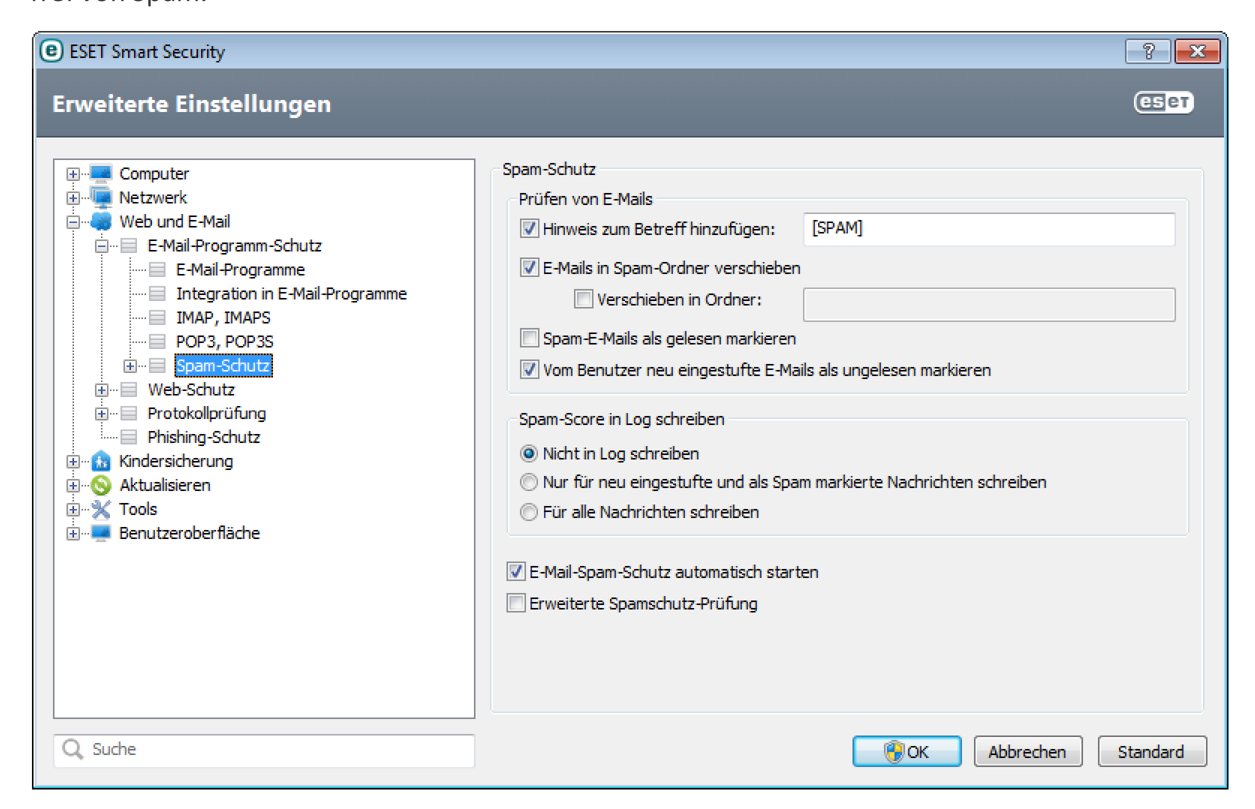
Keine POP3S-Prüfung verwenden - Verschlüsselte Kommunikation wird nicht geprüft

POP3S-Protokollprüfung für ausgewählte Ports durchführen - Die POP3S-Prüfung wird nur für die unter **Portnutzung POP3-Protokoll** festgelegten Ports durchgeführt.

Portnutzung POP3S-Protokoll - Eine Liste zu prüfender POP3S-Ports (standardmäßig 995).

4.3.1.4 Spam-Schutz

Spam, d. h. unerwünschte E-Mails, stellt ein zentrales Problem der elektronischen Kommunikation dar. Spam macht bis zu 80 Prozent der gesamten E-Mail-Kommunikation aus. Der Spam-Schutz nimmt dieses Problem in Angriff. Verschiedene E-Mail-Sicherheitsverfahren sorgen für ausgezeichnete Filterquoten und halten so Ihren Posteingang frei von Spam.



Ein zentrales Prinzip beim Spam-Schutz ist die Möglichkeit der Erkennung unerwünschter E-Mails über eine Positiv- bzw. eine Negativliste. In der Positivliste werden vertrauenswürdige E-Mail-Adressen, in der Negativliste Spam-Adressen vorab definiert. Alle Adressen in Ihrer Kontaktliste sowie alle vom Benutzer als „sicher“ eingestuften Adressen werden automatisch der Positivliste hinzugefügt.

Die primäre Methode zur Spam-Erkennung ist die Prüfung der E-Mail-Eigenschaften. Empfangene Nachrichten werden anhand grundlegender Spam-Kriterien und mithilfe spezifischer Methoden (Nachrichtendefinitionen, statistische Heuristik, Erkennung von Algorithmen usw.) geprüft. Der sich daraus ergebende Indexwert entscheidet darüber, ob eine Nachricht als Spam eingestuft wird oder nicht.

Mit dem Spam-Schutz von ESET Smart Security können Sie für die Verwaltung Ihrer Adresslisten verschiedene Parameter festlegen. Die folgenden Optionen stehen Ihnen zur Verfügung:

Prüfen von E-Mails

Hinweis zum Betreff hinzufügen - Sie können einen Hinweistext festlegen, der zur Betreffzeile von E-Mails hinzugefügt wird, die als Spam eingestuft wurden. Der Standardtext ist „[SPAM]“.

E-Mails in Spam-Ordner verschieben - Wenn diese Option aktiviert ist, werden Spam-E-Mails in den Standard-Spam-Ordner verschoben.

Verschieben in Ordner - Sie können selbst einen Ordner festlegen, in den Spam-E-Mails verschoben werden sollen.

Spam-E-Mails als gelesen markieren - Aktivieren Sie dieses Kontrollkästchen, wenn Spam-E-Mails automatisch als gelesen markiert werden sollen. „Saubere“ Nachrichten sind dann leichter erkennbar.

E-Mails, die vom Benutzer neu eingestuft werden, als ungelesen markieren - Vermeintliche Spam-E-Mails, die Sie manuell als „KEIN Spam“ einstufen, werden als ungelesen markiert.

Spam-Score in Log schreiben

Das Spam-Schutz-Modul von ESET Smart Security berechnet für jede geprüfte Nachricht einen Spam-Score. Die Nachricht wird im Spam-Schutz-Log protokolliert (**ESET Smart Security** > **Tools** > **Log-Dateien** > **Spam-Schutz**).

- **Nicht in Log schreiben** - Die Zelle **Punktzahl** im Log des Spam-Schutzes bleibt leer.
- **Nur für neu eingestufte und als Spam markierte Nachrichten schreiben** - Aktivieren Sie diese Option, wenn Sie eine Spam-Punktzahl für als Spam gekennzeichnete Nachrichten aufzeichnen möchten.
- **Für alle Nachrichten schreiben** - Alle Nachrichten werden im Log mit ihrem Spam-Score protokolliert.

E-Mail-Spam-Schutz automatisch starten - Aktivieren Sie diese Option, um den Spam-Schutz beim Systemstart automatisch zu starten.

Erweiterten Spam-Schutz aktivieren - Aktivieren Sie diese Option, um zusätzliche Spam-Schutz-Datenbanken herunterzuladen. Dies erweitert den Spam-Schutz und ermöglicht bessere Ergebnisse.

ESET Smart Security bietet Spam-Schutz für Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail und Mozilla Thunderbird (bis Version 5).

4.3.1.4.1 Adressen zur Positivliste/Negativliste hinzufügen

E-Mail-Adressen von Personen, mit denen Sie häufig kommunizieren, können in die Positivliste aufgenommen werden. So wird sichergestellt, dass keine Nachricht von einem Absender in der Positivliste als Spam eingestuft wird. Bekannte Spam-E-Mail-Adressen können der Negativliste hinzugefügt und als Spam eingestuft werden. Um der Positiv- bzw. Negativliste eine neue E-Mail-Adresse hinzuzufügen, klicken Sie mit der rechten Maustaste auf die E-Mail und wählen Sie **ESET Smart Security** > **Zur Positivliste hinzufügen** bzw. **Zur Negativliste hinzufügen** oder klicken Sie auf **Vertrauenswürdige Adresse** bzw. **Spam-Adresse** in der Spam-Schutz-Symbolleiste von ESET Smart Security in Ihrem E-Mail-Client.

Bei Spam-Adressen können Sie genauso vorgehen. Jede E-Mail von einer in der Negativliste aufgeführten E-Mail-Adresse wird als Spam eingestuft.

4.3.1.4.2 E-Mails als Spam einstufen

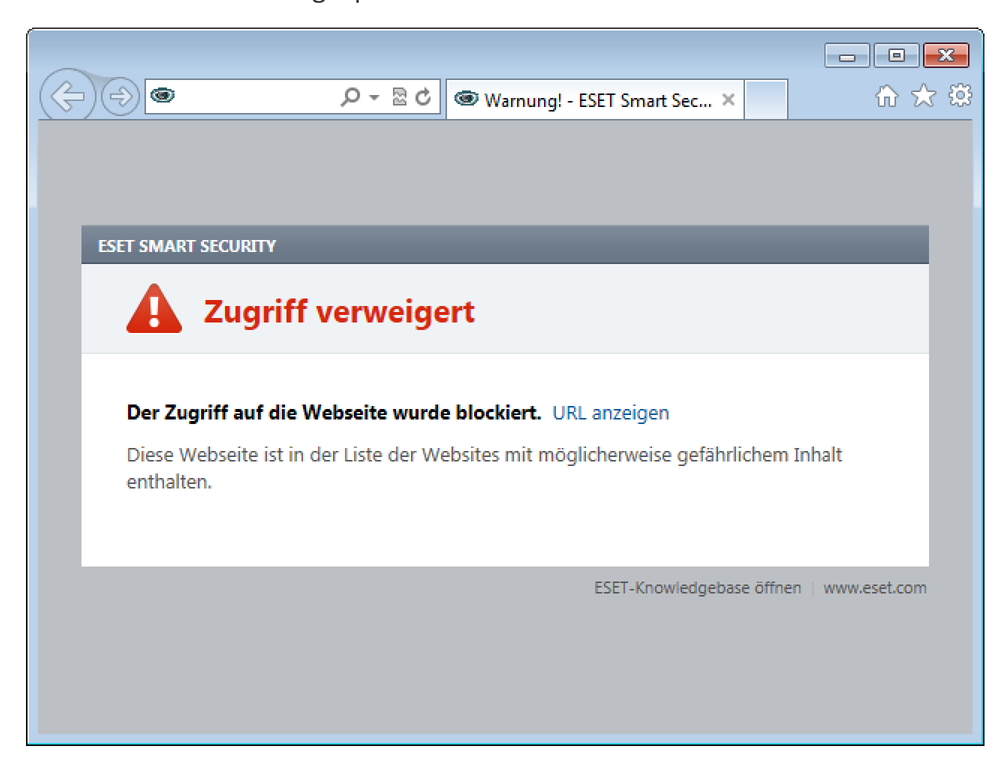
Jede im E-Mail-Programm angezeigte Nachricht kann als Spam eingestuft werden. Klicken Sie dazu mit der rechten Maustaste auf die Nachricht und klicken Sie dann auf **ESET Smart Security** > **Ausgewählte E-Mail(s) als Spam einstufen** oder auf **Spam-Adresse** in der Spam-Schutz-Symbolleiste von ESET Smart Security im oberen Bereich Ihres E-Mail-Programms.

Als Spam eingestufte Nachrichten werden automatisch in den SPAM-Ordner verschoben. Die E-Mail-Adresse des Absenders wird jedoch nicht automatisch in die Negativliste aufgenommen. Gleichermaßen können Sie Nachrichten als „KEIN Spam“ einstufen. Nachrichten aus dem Ordner **Spam-E-Mails** werden in den ursprünglichen Ordner verschoben, wenn sie als „KEIN Spam“ klassifiziert werden. Die E-Mail-Adresse des Absenders wird nicht automatisch in die Positivliste aufgenommen.

4.3.2 Web-Schutz

Der Internetzugang ist eine Standardfunktion von Computern. Leider ist diese technische Möglichkeit mittlerweile auch der wichtigste Weg zur Verbreitung von Schadsoftware. Der Web-Schutz besteht in der Überwachung der Kommunikation zwischen Webbrowsern und Remoteservern und entspricht den Regeln für HTTP (Hypertext Transfer Protocol) und HTTPS (verschlüsselte Kommunikation).

Wir empfehlen dringend, den Web-Schutz zu aktivieren. Zugriff auf diese Option erhalten Sie im Hauptfenster von ESET Smart Security unter **Einstellungen** > **Web und E-Mail** > **Web-Schutz**. Der Zugriff auf bekannte Webseiten mit Schadcode wird immer gesperrt.



4.3.2.1 HTTP, HTTPS

ESET Smart Security ist standardmäßig für die Standards der gängigen Webbrowser konfiguriert. Dennoch können Sie die Einstellungen für die HTTP-Prüfung unter **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **Web-Schutz** > **HTTP, HTTPS** bearbeiten. Im Hauptfenster für die **HTTP/HTTPS-Filterung** können Sie die Option **HTTP-Prüfung aktivieren** aus- bzw. abwählen. Außerdem können Sie die Portnummern für die HTTP-Kommunikation festlegen. In der Standardeinstellung sind die Portnummern 80 (HTTP), 8080 und 3128 (für Proxyserver) vordefiniert.

ESET Smart Security unterstützt die HTTPS-Protokollprüfung. Bei der HTTPS-Kommunikation wird zur Datenübertragung zwischen Server und Client ein verschlüsselter Kanal verwendet. ESET Smart Security überwacht die mit Hilfe der Verschlüsselungsverfahren SSL (Secure Socket Layer) und TLS (Transport Layer Security) abgewickelte Kommunikation. Folgende Optionen stehen für die HTTPS-Prüfung zur Verfügung:

HTTPS-Protokollprüfung nicht verwenden - Verschlüsselte Kommunikation wird nicht geprüft.

HTTPS-Protokollprüfung für ausgewählte Ports durchführen - Es werden nur die Anwendungen geprüft, die im Abschnitt Webbrowser und E-Mail-Programme festgelegt sind und die die unter **Portnutzung HTTPS-Protokoll** festgelegten Ports verwenden. Standardmäßig ist Port 443 eingetragen.

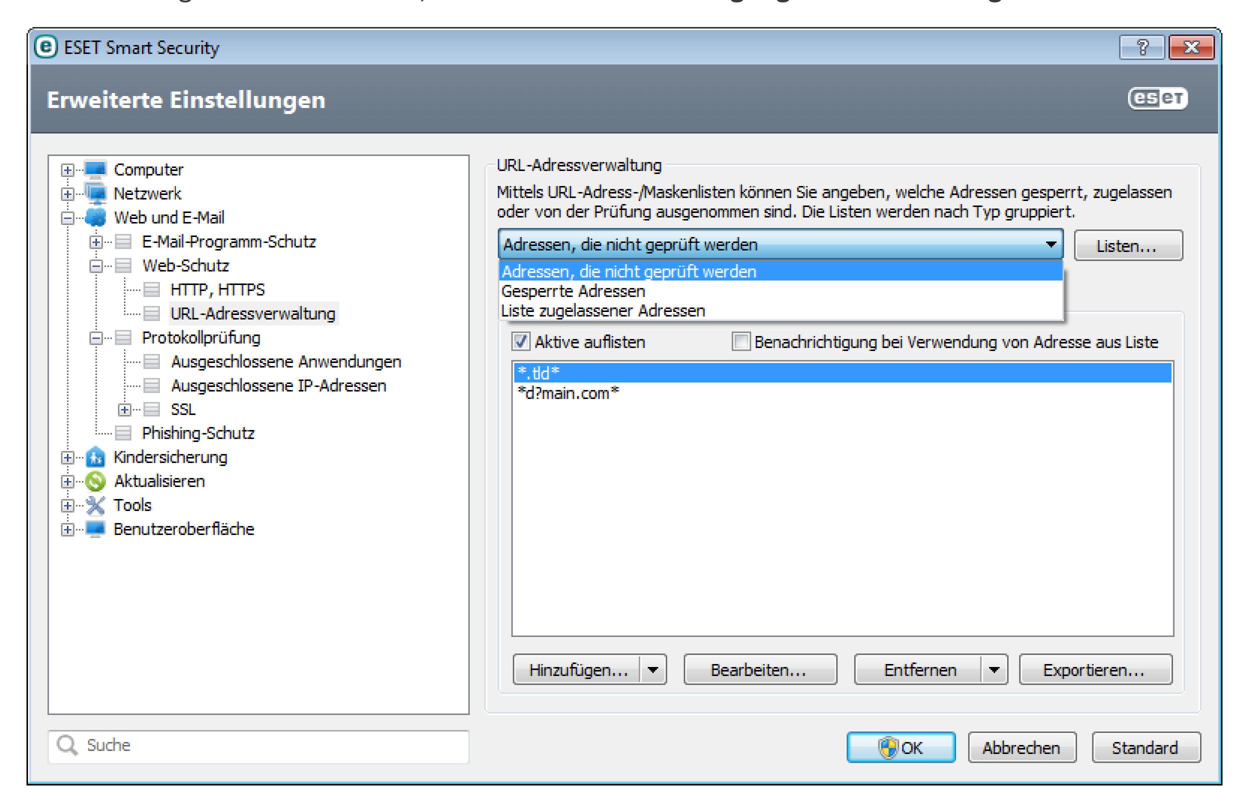
Der Datenverkehr über verschlüsselte Verbindungen wird nicht geprüft. Zur Aktivierung der Prüfung verschlüsselter Verbindungen und zur Anzeige der Prüfeinstellungen navigieren Sie zu SSL-Protokollprüfung in den erweiterten Einstellungen, klicken Sie auf **Web und E-Mail** > **Prüfen von Anwendungsprotokollen** > **SSL** und aktivieren Sie die Option **SSL-Protokoll immer prüfen**.

4.3.2.2 URL-Adressverwaltung

Im Bereich URL-Adressverwaltung können Sie festlegen, welche HTTP-Adressen blockiert, zugelassen oder von der Prüfung ausgeschlossen werden sollen. Mit den Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Exportieren** können Sie die Adresslisten verwalten. Auf Websites, die in der Liste der blockierten Adressen aufgeführt sind, ist kein Zugriff möglich. Websites, die in der Liste der ausgeschlossenen Websites aufgeführt sind, werden vor dem Zugriff nicht auf Schadcode überprüft. Durch Aktivierung der Option **Nur Zugriff auf URL-Adressen aus der Liste zulässiger Adressen erlauben** können Sie nur auf Adressen in dieser Liste zugreifen, während alle anderen HTTP-Adressen gesperrt werden.

Wenn Sie eine URL-Adresse zur Liste **Adressen, die nicht geprüft werden** hinzufügen, wird diese von der Prüfung ausgenommen. Sie können auch bestimmte Adressen zulassen oder sperren, indem Sie sie zur **Liste zugelassener Adressen** oder zu **Gesperrte Adressen** hinzufügen. Klicken Sie zum Öffnen des Fensters **HTTP-Adress-/Maskenlisten** auf **Listen...**. Dort können Sie Adresslisten **Hinzufügen** oder **Entfernen**. Um eine HTTPS-URL-Adresse zu der Liste hinzufügen zu können, muss die Option **SSL-Protokoll immer prüfen** aktiviert sein.

In allen Listen können Sie die Platzhalterzeichen * (Sternchen) und ? (Fragezeichen) verwenden. Das Sternchen ersetzt eine beliebige Zeichenfolge, das Fragezeichen ein beliebiges Symbol. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie darauf, dass die Zeichen „*“ und „?“ korrekt verwendet werden. Um eine Liste zu aktivieren, wählen Sie die Option **Liste aktiv**. Wenn Sie beim Zugriff auf eine Adresse aus der aktuellen Liste benachrichtigt werden möchten, wählen Sie **Benachrichtigung bei Verwendung von Adresse aus Liste**.



Hinzufügen/Aus Datei - Hiermit können Sie der Liste entweder manuell (**Hinzufügen**) oder aus einer einfachen Textdatei (**Aus Datei**) eine Adresse hinzufügen. Die Option **Aus Datei** ermöglicht Ihnen das Hinzufügen mehrerer URL-Adressen/-Masken, die in einer Textdatei gespeichert sind.

Bearbeiten...- Adressen manuell bearbeiten, z. B. durch Hinzufügen eines Platzhalters („*“ und „?“).

Entfernen/Alle entfernen - Klicken Sie auf **Entfernen**, um die ausgewählte Adresse aus der Liste zu löschen. Klicken Sie auf **Alle entfernen**, um alle Adressen zu löschen.

Exportieren... - Adressen aus der aktuellen Liste in einer einfachen Textdatei speichern.

4.3.3 Prüfen von Anwendungsprotokollen

Das ThreatSense-Prüfmodul, in dem alle erweiterten Prüfmethoden integriert sind, bietet Virenschutz für Anwendungsprotokolle. Die Prüfung ist unabhängig vom eingesetzten E-Mail-Programm oder Webbrowser. Informationen zur verschlüsselten (SSL-)Kommunikation finden Sie unter **Prüfen von Anwendungsprotokollen** > **SSL**.

Prüfen von anwendungsspezifischen Protokollen aktivieren - Wenn diese Option aktiviert ist, wird die gesamte Kommunikation über HTTP(S), POP3(S) und IMAP(S) geprüft.

HINWEIS: Ab Windows Vista Service Pack 1, Windows 7 und Windows Server 2008 wird zur Prüfung der Netzwerkkommunikation die neue Architektur der Windows-Filterplattform (WFP) verwendet. Da bei der WFP-Technologie spezielle Überwachungstechniken verwendet werden, stehen die folgenden Optionen nicht zur Verfügung:

- **HTTP-, POP3 und IMAP-Ports** - Beschränkt die Weiterleitung zum internen Proxyserver auf die entsprechenden Ports
- **Als Webbrowser oder E-Mail-Programme eingestufte Anwendungen** - beschränkt die Weiterleitung zum internen Proxyserver auf Anwendungen, die als Webbrowser oder E-Mail-Programme eingestuft sind (**Web und E-Mail** > **Prüfen von Anwendungsprotokollen** > **Webbrowser und E-Mail-Programme**).
- **Als Webbrowser oder E-Mail-Programme eingestufte Ports und Anwendungen** - Aktiviert die Weiterleitung des Datenverkehrs von den entsprechenden Ports sowie von Anwendungen, die als Webbrowser oder E-Mail-Programme eingestuft sind, an den internen Proxyserver.

4.3.3.1 Webbrowser und E-Mail-Programme

HINWEIS: Ab Windows Vista Service Pack 1 und Windows Server 2008 wird zur Prüfung der Netzwerkkommunikation die neue Architektur der Windows-Filterplattform (WFP) verwendet. Da bei der WFP-Technologie spezielle Überwachungstechniken verwendet werden, steht hier der Abschnitt **Webbrowser und E-Mail-Programme** nicht zur Verfügung.

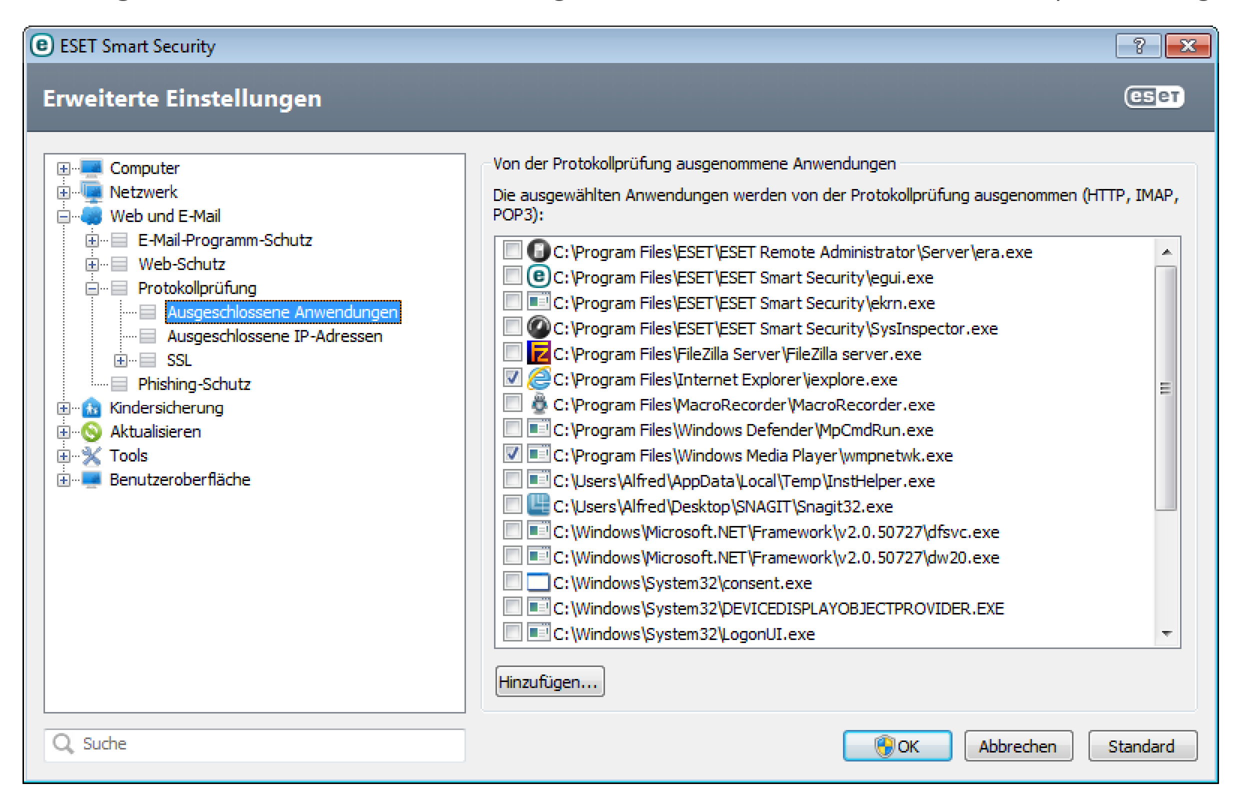
Da im Internet Sicherheitsbedrohungen allgegenwärtig sind, ist sicheres Internetsurfen besonders wichtig. Durch Sicherheitslücken in Webbrowsern und gefälschte Hyperlinks kann Schadcode unbemerkt in Ihr System eindringen. Deshalb bietet ESET Smart Security besondere Funktionen zur Verbesserung der Sicherheit von Webbrowsern an. Sie können beliebige Anwendungen, die auf das Internet zugreifen, als Webbrowser einstufen. Das Kontrollkästchen kann einen der zwei folgenden Status annehmen:

- **Nicht aktiviert** - Die Kommunikation der Anwendungen wird nur für festgelegte Ports gefiltert.
- **Aktiviert** - Die Kommunikation der Anwendungen wird immer geprüft (auch wenn ein anderer Port angegeben ist).

4.3.3.2 Ausgeschlossene Anwendungen

Wählen Sie aus der Liste die Netzwerk-Anwendungen, für deren Datenkommunikation keine Inhaltsprüfung erfolgen soll. Dies schließt die HTTP/POP3/IMAP-Datenkommunikation ausgewählter Anwendungen von der Prüfung auf Bedrohungen aus. Wir empfehlen, diese Option nur für Anwendungen zu aktivieren, deren Datenkommunikation nicht ordnungsgemäß funktioniert, wenn die Prüfung aktiviert ist.

Aktuell ausgeführte Anwendungen und Dienste stehen hier automatisch zur Verfügung. Klicken Sie auf **Hinzufügen...**, um manuell eine Anwendung auszuwählen, die nicht in der Protokollprüfliste angezeigt wird.

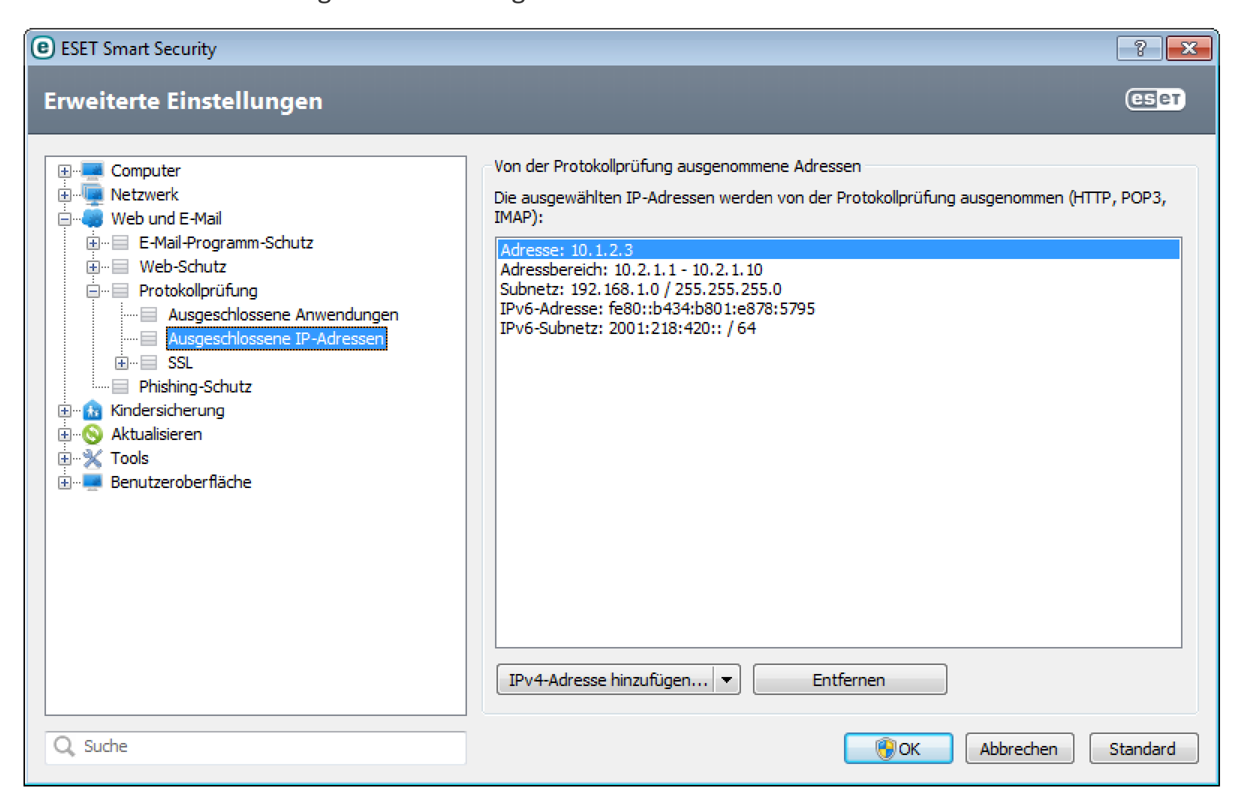


4.3.3.3 Ausgeschlossene IP-Adressen

Die in der Liste eingetragenen Adressen werden von der Protokollinhaltsprüfung ausgeschlossen. Die HTTP/POP3/IMAP-Datenkommunikation von/an die ausgewählten Adressen wird nicht auf Bedrohungen geprüft. Wir empfehlen, diese Option nur für Adressen zu aktivieren, die als vertrauenswürdig bekannt sind.

IPv4/IPv6-Adresse hinzufügen - Hier können Sie eine IP-Adresse, einen Bereich von Adressen oder ein Subnetz für die Gegenstelle festlegen, die von der Regel erfasst wird.

Entfernen - Entfernt ausgewählte Einträge aus der Liste.



4.3.3.3.1 IPv4-Adresse hinzufügen

Hier können Sie eine IP-Adresse, einen Bereich von Adressen oder ein Subnetz für die Gegenstelle festlegen, die von der Regel erfasst wird. Version 4 ist eine ältere Version des Internetprotokolls. Nach wie vor hat diese Version jedoch die größte Verbreitung.

Einzelne Adresse - Hinzufügen der IP-Adresse eines einzelnen Computers, auf den die Regel angewendet werden soll (zum Beispiel *192.168.0.10*).

Adressbereich - Geben Sie die Start- und Endadresse eines Bereichs von IP-Adressen ein (von mehreren Computern), auf die die Regel angewendet werden soll (z. B. *192.168.0.1* bis *192.168.0.99*).

Subnetz - Hier können Sie durch eine IP-Adresse und eine Maske ein Subnetz (eine Gruppe von Computern) definieren.

255.255.255.0 ist z. B. die Netzwerkmaske für das Präfix *192.168.1.0/24*, also der Adressbereich *192.168.1.1* bis *192.168.1.254*.

4.3.3.3.2 IPv6-Adresse hinzufügen

Hier können Sie eine IPv6-Adresse/ein IPv6-Subnetz für die Gegenstelle festlegen, auf die die Regel angewendet werden soll. IPv6 ist die neueste Version des Internetprotokolls, und wird die bisherige Version 4 ersetzen.

Einzelne Adresse - Hier können Sie die IP-Adresse eines einzelnen Computers eingeben, auf den die Regel angewendet werden soll (z. B. *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subnetz - Hier können Sie durch eine IP-Adresse und eine Maske ein Subnetz definieren. (Beispiel: *2002:c0a8:6301:1::1/64*)

4.3.3.4 SSL-Protokollprüfung

Mit ESET Smart Security können Sie Protokolle prüfen, die im SSL-Protokoll gekapselt sind. Für durch SSL geschützte Kommunikation gibt es verschiedene Prüfmodi mit vertrauenswürdigen und unbekannten Zertifikaten sowie Zertifikaten, die von der Prüfung SSL-geschützter Kommunikation ausgeschlossen sind.

SSL-Protokoll immer prüfen - Aktivieren Sie diese Option, um jegliche SSL-geschützte Kommunikation zu prüfen (außer wenn Zertifikate verwendet werden, die von der Prüfung ausgeschlossen sind). Wird eine Verbindung mit einem unbekannten, signierten Zertifikat erstellt, so wird sie ohne gesonderten Hinweis automatisch geprüft. Wenn Sie auf einen Server mit einem nicht vertrauenswürdigen Zertifikat, das Sie zur Liste der vertrauenswürdigen Zertifikate hinzugefügt und damit als vertrauenswürdig eingestuft haben, zugreifen, wird die Kommunikation zugelassen und der Inhalt des Kommunikationskanals geprüft.

Nach nicht besuchten Websites fragen (es können Ausschlüsse festgelegt werden) - Wenn Sie auf eine neue durch SSL geschützte Website (mit einem unbekannten Zertifikat) zugreifen, wird eine Aktionsauswahl angezeigt. In diesem Modus können Sie eine Liste von SSL-Zertifikaten erstellen, die von der Prüfung ausgeschlossen sind.

SSL-Protokoll nicht prüfen - Ist diese Option aktiviert, prüft das Programm keine Kommunikation via SSL.

Erstellte Ausnahmen auf der Basis von Zertifikaten übernehmen - Aktiviert die Verwendung von Ausnahmen, die in den Listen für ausgeschlossene und vertrauenswürdige Zertifikate festgelegt sind, zur Prüfung von SSL-Verbindungen. Diese Option ist verfügbar, wenn Sie **SSL-Protokoll immer prüfen** wählen.

Verschlüsselte Kommunikation sperren, die das obsolete Protokoll SSL v2 verwendet - Verbindungen, die die frühere Version des SSL-Protokolls verwenden, werden automatisch blockiert.

4.3.3.4.1 Zertifikate

Damit die SSL-Kommunikation in Ihren Browsern/E-Mail-Programmen ordnungsgemäß funktioniert, muss das Stammzertifikat für ESET der Liste der bekannten Stammzertifikate (Herausgeber) hinzugefügt werden. **Bekannten Browsern das Stammzertifikat hinzufügen** sollte aktiviert sein. Wählen Sie diese Option, um das ESET-Stammzertifikat automatisch zu den bekannten Browsern (z. B. Opera, Firefox) hinzuzufügen. Wenn ein Browser den Systemzertifizierungsspeicher verwendet, wird das Zertifikat automatisch hinzugefügt (z. B. Internet Explorer). Um das Zertifikat für nicht unterstützte Browser zu übernehmen, klicken Sie auf **Zertifikat anzeigen** > **Details** > **In die Datei kopieren...**, und importieren Sie es anschließend manuell in den Browser.

In manchen Fällen kann das Zertifikat nicht über den Speicher vertrauenswürdiger Stammzertifizierungsstellen geprüft werden (z. B. VeriSign). Das bedeutet, dass jemand das Zertifikat selbst signiert hat (z. B. der Administrator eines Webservers oder ein Kleinunternehmen). Das Zertifikat als vertrauenswürdig einzustufen, stellt nicht immer ein Risiko dar. Die meisten großen Unternehmen (z. B. Banken) verwenden Zertifikate, die von einer vertrauenswürdigen Stammzertifizierungsstelle signiert sind. Wenn die Option **Gültigkeit des Zertifikats erfragen** ausgewählt ist (Standardeinstellung), muss der Benutzer eine Aktion festlegen, die ausgeführt werden soll, wenn verschlüsselte Verbindungen aufgebaut werden. Dazu wird ein Aktionsauswahl-Dialogfenster angezeigt, in dem Sie das Zertifikat als vertrauenswürdig markieren oder ausschließen können. Wenn das Zertifikat nicht in der Liste vertrauenswürdiger Stammzertifizierungsstellen enthalten ist, ist das Fenster rot hinterlegt, sonst ist es grün.

Sie können die Option **Kommunikation blockieren, die das Zertifikat verwendet** auswählen, um verschlüsselte Verbindungen zu der Site, die das nicht verifizierte Zertifikat verwendet, immer zu beenden.

Wenn das Zertifikat ungültig oder beschädigt ist, ist es entweder abgelaufen oder wurde fehlerhaft selbst signiert.

In diesem Fall empfehlen wir, die Verbindung, die das Zertifikat verwendet, zu blockieren.

4.3.3.4.1.1 Vertrauenswürdige Zertifikate

Neben dem integrierten Speicher vertrauenswürdiger Stammzertifizierungsstellen, in dem ESET Smart Security vertrauenswürdige Zertifikate speichert, können diese außerdem in einer benutzerdefinierten Liste abgelegt werden. Über **Erweiterte Einstellungen** (F5) > **Web und E-Mail** > **Prüfen von Anwendungsprotokollen** > **SSL** > **Zertifikate** > **Vertrauenswürdige Zertifikate** können Sie sich diese Liste anzeigen lassen. ESET Smart Security prüft den Inhalt verschlüsselter Verbindungen mithilfe der in dieser Liste enthaltenen Zertifikate.

Klicken Sie auf **Entfernen**, um die ausgewählten Elemente aus der Liste zu entfernen. Klicken Sie auf **Anzeigen** (oder doppelklicken Sie auf das Zertifikat), um Informationen zum ausgewählten Zertifikat anzuzeigen.

4.3.3.4.1.2 Ausgeschlossene Zertifikate

Der Bereich „Ausgeschlossene Zertifikate“ enthält Zertifikate, die als sicher gelten. Das Programm prüft den Inhalt verschlüsselter Verbindungen, die ein in dieser Liste enthaltenes Zertifikat verwenden, nicht auf Bedrohungen. Es wird empfohlen, nur garantiert sichere Webzertifikate auszuschließen, sodass die Verbindungen mithilfe dieser Zertifikate nicht geprüft werden müssen. Klicken Sie auf **Entfernen**, um die ausgewählten Elemente aus der Liste zu entfernen. Klicken Sie auf **Anzeigen** (oder doppelklicken Sie auf das Zertifikat), um Informationen zum ausgewählten Zertifikat anzuzeigen.

4.3.3.4.1.3 Verschlüsselte SSL-Kommunikation

Falls der Computer für SSL-Protokollüberprüfung eingerichtet ist, werden Sie in einem Dialogfenster aufgefordert, eine Aktion auszuwählen, die verwendet wird, sobald eine verschlüsselte Kommunikation (über ein unbekanntes Zertifikat) angefordert wird. Folgende Daten werden angezeigt: Der Name der Anwendung, die die Kommunikation einleitete, sowie der Name des verwendeten Zertifikats.

Befindet sich das Zertifikat nicht im Speicher vertrauenswürdiger Stammzertifizierungsstellen, wird es als nicht vertrauenswürdig erachtet.

Für Zertifikate stehen folgende Aktionen zur Verfügung:

Ja - Das Zertifikat wird vorübergehend für die aktuelle Sitzung als vertrauenswürdig gekennzeichnet; beim nächsten Versuch, das Zertifikat zu verwenden, wird keine Warnung angezeigt.

Ja, immer - Das Zertifikat wird als vertrauenswürdig gekennzeichnet und zur Liste vertrauenswürdiger Zertifikate hinzugefügt; für vertrauenswürdige Zertifikate werden keine Warnungen angezeigt.

Nein - Das Zertifikat wird für die aktuelle Sitzung als nicht vertrauenswürdig gekennzeichnet; beim nächsten Versuch, das Zertifikat zu verwenden, wird erneut eine Warnung angezeigt.

Ausschließen - Das Zertifikat wird zur Liste ausgeschlossener Zertifikate hinzugefügt; es findet keine Prüfung des über einen verschlüsselten Kanal übertragenen Datenverkehrs statt.

4.3.4 Phishing-Schutz

Der Begriff „Phishing“ bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Phishing wird oft eingesetzt, um Zugriff auf vertrauliche Daten zu erlangen, wie Kontonummern oder PIN-Codes. Weitere Informationen zu dieser Aktivität finden Sie im Glossar. ESET Smart Security bietet Phishing-Schutz: Webseiten, die dafür bekannt sind, Phishing-Inhalte zu enthalten, können gesperrt werden.

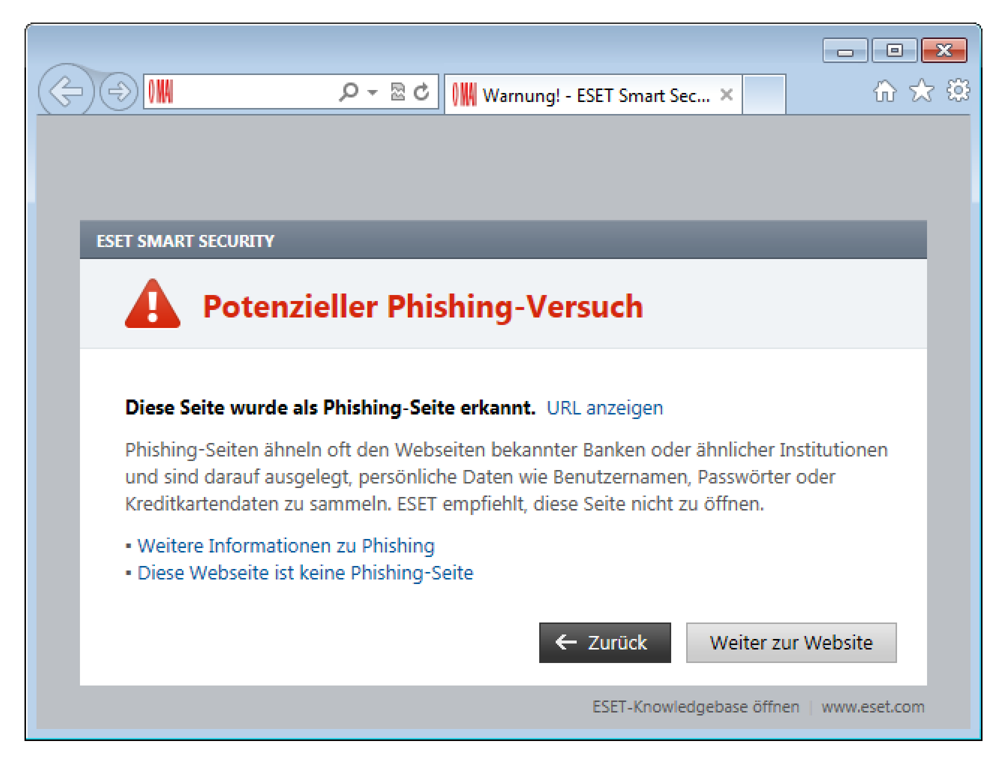
Wir empfehlen, den Phishing-Schutz in ESET Smart Security zu aktivieren. Diese Option finden Sie im Bereich **Einstellungen** (F5) unter **Web und E-Mail** > **Phishing-Schutz**.

Eine aktualisierte und detaillierte Version dieser Hilfeseite finden Sie im folgenden Knowledgebase-Artikel.

Zugriff auf eine Phishing-Website

Wenn Sie auf eine Phishing-Website zugreifen, wird das nachfolgend abgebildete Dialogfenster im Webbrowser

angezeigt. Wenn Sie auf **Weiter zur Website** klicken (nicht empfohlen), können Sie ohne Warnmeldung auf die Website zugreifen.



HINWEIS: Potenzielle Phishing-Websites, die zur Positivliste hinzugefügt wurden, werden standardmäßig nach einigen Stunden wieder von der Liste gelöscht. Verwenden Sie die URL-Adressverwaltung, um eine Website dauerhaft zuzulassen. Klicken Sie unter **Erweiterte Einstellungen** (F5) auf **Web und E-Mail** > **Web-Schutz** > **URL-Adressverwaltung**, wählen Sie in der Auswahlliste **URL-Adressverwaltung** die Option **Liste zugelassener Adressen** aus und fügen Sie Ihre Webseite zu dieser Liste hinzu.

Melden einer Phishing-Website

Über den Link Phishing-Website melden können Sie eine Website mit vermutetem Phishing-Inhalt oder anderem Schadcode bei ESET melden.

HINWEIS: Auf Websites, die Sie bei ESET melden, sollte mindestens eines der folgenden Kriterien zutreffen:
- Die Website wird nicht als Bedrohung erkannt.
- Die Website wird als Bedrohung erkannt, obwohl Sie keinen Schadcode enthält. Beachten Sie in diesem Fall die Informationen unter Phishing-Website entfernen.

Sie können Websites auch per E-Mail melden. Senden Sie die E-Mail an samples@eset.com. Verwenden Sie einen treffenden Text in der Betreffzeile und fügen Sie möglichst viele Informationen zur Website ein (wie Sie auf die Website gelangt sind, wo Sie von der Website gehört haben usw.).

4.4 Kindersicherung

Im Modul „Kindersicherung“ können Sie die Einstellungen für diese Option wählen. So haben Eltern die Möglichkeit, ihre Kinder mit automatisierten Funktionen zu schützen und die Benutzung von Geräten und Diensten einzuschränken. Ziel ist es, dass Kinder und Jugendliche keinen Zugriff auf Websites mit ungeeigneten oder schädlichen Inhalten erhalten.

Mit der Kindersicherung können Sie Webseiten sperren, die potenziell Unerlaubtes enthalten könnten. Außerdem können Eltern mit dieser Funktion den Zugriff auf über 40 vordefinierte Webseitenkategorien und über 140 Unterkategorien unterbinden.

Befolgen Sie die nachstehenden Schritte, um die Kindersicherung für ein bestimmtes Benutzerkonto zu aktivieren:

1. Standardmäßig ist die Kindersicherung in ESET Smart Security deaktiviert. Zur Aktivierung der Kindersicherung stehen zwei Methoden zur Verfügung:

- o Klicken Sie im Hauptprogrammfenster im Bereich **Einstellungen** auf **Deaktiviert** und ändern Sie den Status der Kindersicherung zu **Aktiviert**.
- o Drücken Sie F5, um die **Erweiterten Einstellungen** zu öffnen. Wählen Sie dann **Kindersicherung** aus und aktivieren Sie das Kontrollkästchen neben **Systemintegration**.

2. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Kindersicherung**. Auch wenn bereits **Aktiviert** neben dem Eintrag **Kindersicherung** angezeigt wird, müssen Sie die Kindersicherung für das gewünschte Konto zunächst durch Klicken auf **Nicht definiert** konfigurieren. Geben Sie im Kontoeinrichtungsfenster ein Alter ein, um die Zugriffsebene und empfohlene, altersangemessene Webseiten zu bestimmen. Die Kindersicherung wird nun für das angegebene Benutzerkonto aktiviert. Klicken Sie unter dem Kontonamen auf **Einstellungen**, um auf der Registerkarte Inhaltsprüfung für Webseiten Kategorien festzulegen, die Sie blockieren bzw. zulassen möchten. Um Webseiten zu blockieren bzw. zuzulassen, die keiner Kategorie entsprechen, klicken Sie auf die Registerkarte Gesperrte und zugelassene Webseiten.



Wenn Sie auf den Titel **Kindersicherung** im Bereich **Einstellungen** des Hauptprogrammfensters von ESET Smart Security klicken, sehen Sie ein in drei Abschnitte unterteiltes Hauptfenster.

1. Kindersicherung

Wenn Sie rechts die Auswahl der Option **Aktiviert** aufheben, wird das Fenster **Schutz vorübergehend deaktivieren** angezeigt. In diesem Fenster können Sie den Zeitraum festlegen, für den der Schutz deaktiviert werden soll. Die Option wechselt dann zu **Deaktiviert** und alle folgenden Einstellungen werden ausgeblendet.

Es ist wichtig, die Einstellungen von ESET Smart Security mit einem Passwort zu schützen. Dieses Passwort können Sie im Bereich Einstellungen für den Zugriff festlegen. Wenn kein Passwort festgelegt ist, erscheint unter der Option **Kindersicherung** der Warnhinweis Zum Schutz vor Änderungen an den erweiterten Einstellungen ist ein Passwort erforderlich und **Passwort festlegen...** wird angezeigt. Die in der Kindersicherung festgelegten Einschränkungen betreffen nur die Konten von Standardbenutzern. Auf Administratorkonten haben sie keine Auswirkungen, da diese umfassende Rechte haben.

Standardmäßig wird HTTPS (SSL)-Kommunikation nicht gefiltert. Daher kann keine Sperre für Webseiten festgelegt werden, deren Adresse mit *https://* beginnt. Um diese Funktion zu aktivieren, wählen Sie **Aktivieren** neben dem

Das Filtern verschlüsselter Websites (HTTPS) ist nicht aktiviert-Warnhinweis oder wählen Sie **SSL-Protokoll immer prüfen** im Bereich **Erweiterte Einstellungen** > **Web und E-Mail** > **Prüfen von Anwendungsprotokollen** > **SSL**.

Hinweis: Damit die Kindersicherung ordnungsgemäß funktioniert, müssen das Prüfen von anwendungsspezifischen Protokollen, die HTTP-Prüfung und die Systemintegration der Personal Firewall aktiviert sein. Diese Funktionen sind standardmäßig aktiviert.

2. Windows-Benutzerkonten

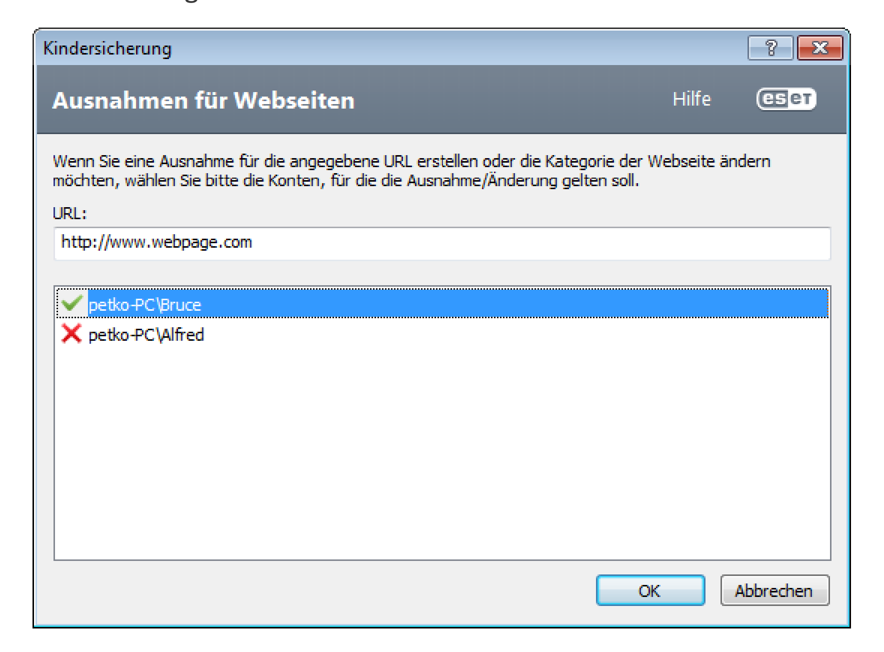
Wenn Sie eine Rolle für ein vorhandenes Konto erstellt haben, wird es hier mit dem Attribut **Aktiviert** angezeigt. Durch Klicken auf **Aktiviert** wird der Status der Kindersicherung für das Konto gewechselt. Klicken Sie unter einem aktiven Konto auf **Konfigurieren...**, um die Liste der zugelassenen Webseiten-Kategorien, die gesperrten und die zugelassenen Webseiten für das Konto anzuzeigen.

Wichtig: Führen Sie folgende Schritte aus, um unter Windows 7 oder Windows Vista ein neues Konto (z. B. für ein Kind) zu erstellen:

1. Öffnen Sie das Fenster Benutzerkonten. Klicken Sie hierzu auf die Schaltfläche **Start** (am unteren linken Bildschirmrand), auf den Eintrag **Systemsteuerung** und dann auf **Benutzerkonten**.
2. Klicken Sie auf **Anderes Konto verwalten**. Wenn Sie zur Eingabe des Administratorpassworts oder zu einer Bestätigung aufgefordert werden, geben Sie das Passwort ein bzw. bestätigen Sie.
3. Klicken Sie auf **Neues Konto erstellen**.
4. Geben Sie den gewünschten Namen für das Benutzerkonto an, klicken Sie auf den gewünschten Kontotyp und klicken Sie dann auf **Konto erstellen**.
5. Öffnen Sie erneut den Bereich „Kindersicherung", indem Sie im Hauptprogrammfenster von ESET Smart Security auf **Erweiterte Einstellungen** > **Kindersicherung** klicken.

3. Der letzte Fensterbereich enthält zwei Optionen

Ausnahme für Webseite festlegen - Mit dieser Option können Sie für das ausgewählte Konto schnell eine Ausnahme für eine Webseite festlegen. Geben Sie die URL-Adresse der Webseite in das Feld **URL** ein und wählen Sie das Konto aus der nachstehenden Liste aus. Wenn Sie das Kontrollkästchen **Sperren** aktivieren, wird diese Webseite für dieses Konto gesperrt. Wenn Sie das Kontrollkästchen nicht aktivieren, wird der Zugriff auf die Webseite zugelassen.

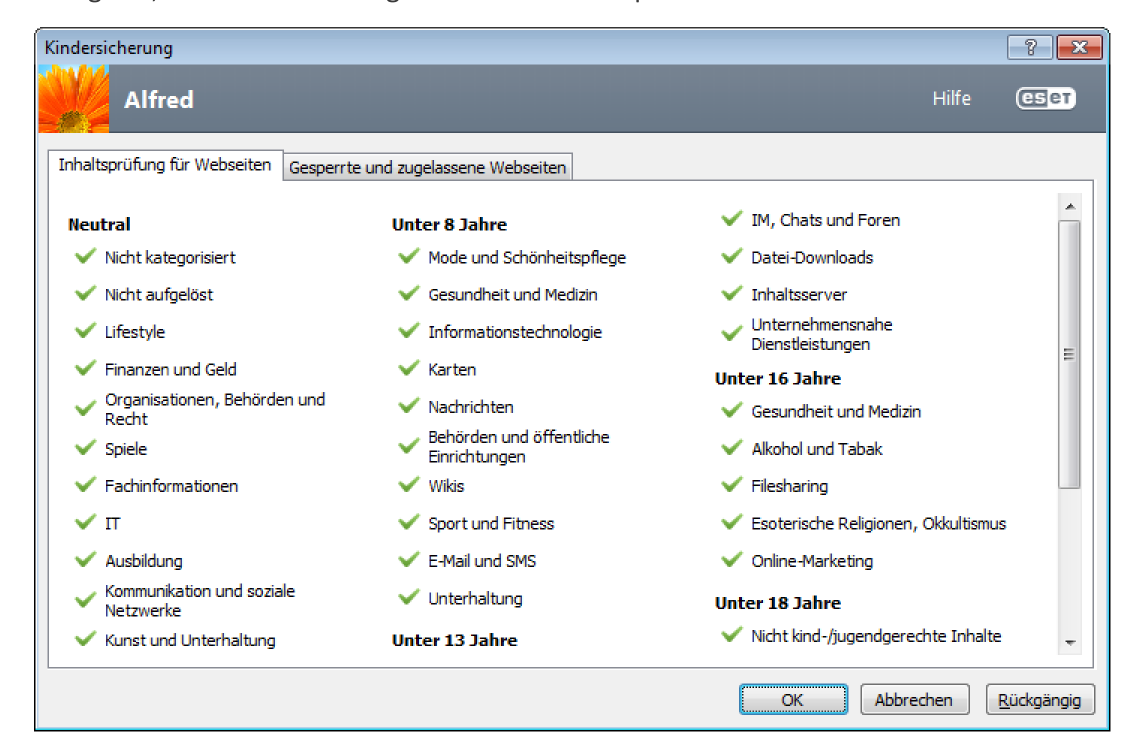


Die hier festgelegten Ausnahmen haben Vorrang vor den Kategorien, die für die ausgewählten Konten festgelegt wurden. Ist für ein Konto zum Beispiel die Kategorie **Nachrichten** gesperrt, doch Sie lassen eine bestimmte Nachrichten-Webseite als Ausnahme zu, kann das Konto auf diese nun zugelassene Webseite zugreifen. Hier festgelegte Änderungen können Sie unter Gesperrte und zugelassene Webseiten überprüfen.

Log anzeigen - Es wird ein detailliertes Log über die Aktivitäten der Kindersicherung angezeigt (gesperrte Webseiten, das Konto, dem der Zugriff auf die Webseite verweigert wurde, der Grund usw.). Sie können dieses Log auch nach gewünschten Kriterien filtern, indem Sie auf **Filter...** klicken.

4.4.1 Prüfen von Webseiteninhalten

Kategorien mit aktiviertem Kontrollkästchen werden zugelassen. Deaktivieren Sie das Kontrollkästchen neben der Kategorie, um sie für das ausgewählte Konto zu sperren.

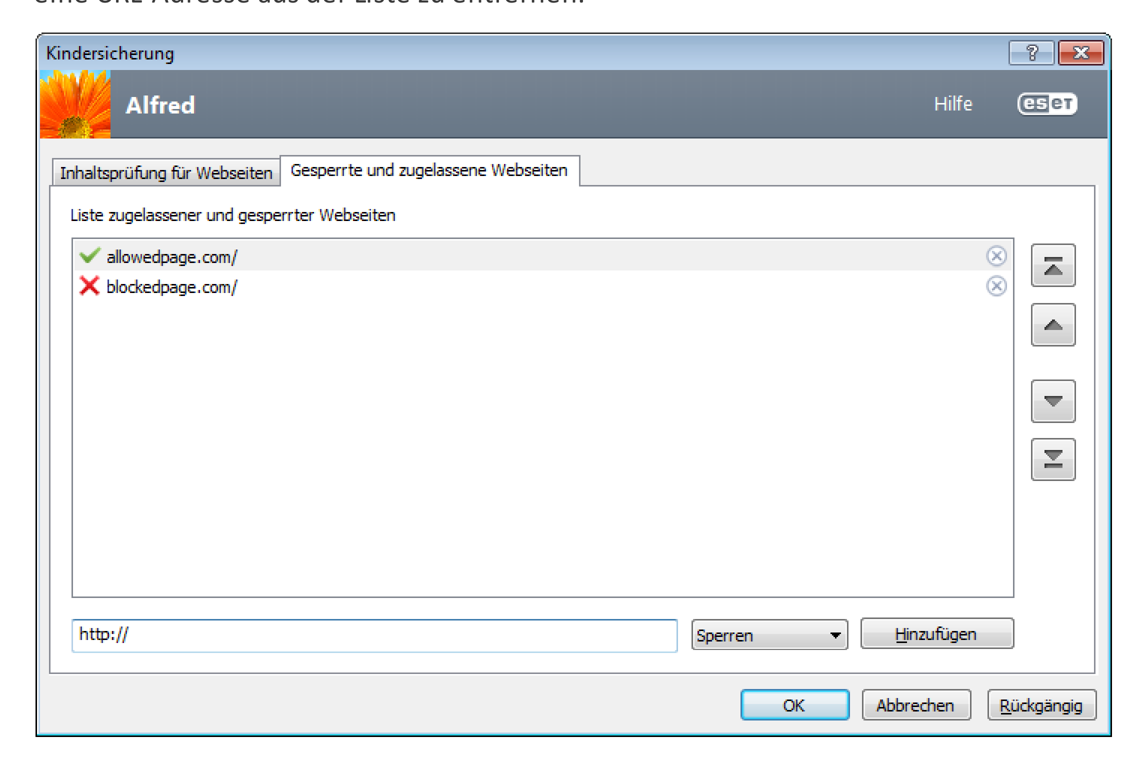


Bewegen Sie den Mauszeiger über eine Kategorie, um sich die entsprechende Liste mit Webseiten anzeigen zu lassen. Nachfolgend finden Sie einige Beispiele für Kategorien (Gruppen), mit denen der Benutzer möglicherweise nicht vertraut ist.

- **Allgemein** - Üblicherweise private (lokale) IP-Adressen, z. B. Intranet, 127.0.0.0/8, 192.168.0.0/16 usw. Bei einem Fehlercode 403 oder 404 wird die Website ebenfalls in diese Kategorie eingestuft.
- **Nicht augelöst** - Diese Kategorie enthält Webseiten, die aufgrund eines Fehlers bei der Verbindung zur Datenbank-Engine der Kindersicherung nicht aufgelöst werden konnten.
- **Nicht kategorisiert** - Unbekannte Webseiten, die noch nicht in der Datenbank der Kindersicherung enthalten sind.
- **Proxys** - Webseiten mit Funktionen zur Anonymisierung oder Umleitung oder öffentliche Proxyserver können dazu eingesetzt werden, um (anonym) auf Webseiten zuzugreifen, die üblicherweise durch die Kindersicherung gesperrt werden.
- **Dateifreigabe** - Webseiten dieser Kategorie enthalten große Mengen Daten, beispielsweise Fotos, Videos oder E-Books. Es besteht die Gefahr, dass eine solche Website potenziell unerlaubte Inhalte enthält.

4.4.2 Gesperrte und zugelassene Webseiten

Geben Sie im leeren Feld unterhalb der Liste eine URL-Adresse ein und wählen Sie **Zulassen** oder **Sperren** aus. Klicken Sie dann auf **Hinzufügen**, um die Adresse zur Liste hinzuzufügen. Klicken Sie auf die Schaltfläche ⊗, um eine URL-Adresse aus der Liste zu entfernen.



In der Liste der URL-Adressen können Sie die Sonderzeichen * (Sternchen) und ? (Fragezeichen) nicht verwenden. Webseitenadressen mit mehreren TLDs müssen beispielsweise manuell eingegeben werden *(beispielseite.com*, *beispielseite.sk* usw.). Wenn Sie eine Domäne zur Liste hinzufügen, werden alle Inhalte der Domäne und der Unterdomänen (z. B. *unterdomäne.beispielseite.com*) je nach gewählter URL-basierter Aktion gesperrt bzw. zugelassen.

Hinweis: Eine bestimmte Webseite zu sperren bzw. zuzulassen kann effizienter sein, als dies für eine ganze Kategorie von Webseiten zu tun. Seien Sie vorsichtig, wenn Sie diese Einstellungen ändern oder eine Kategorie/ Webseite zu einer Liste hinzufügen.

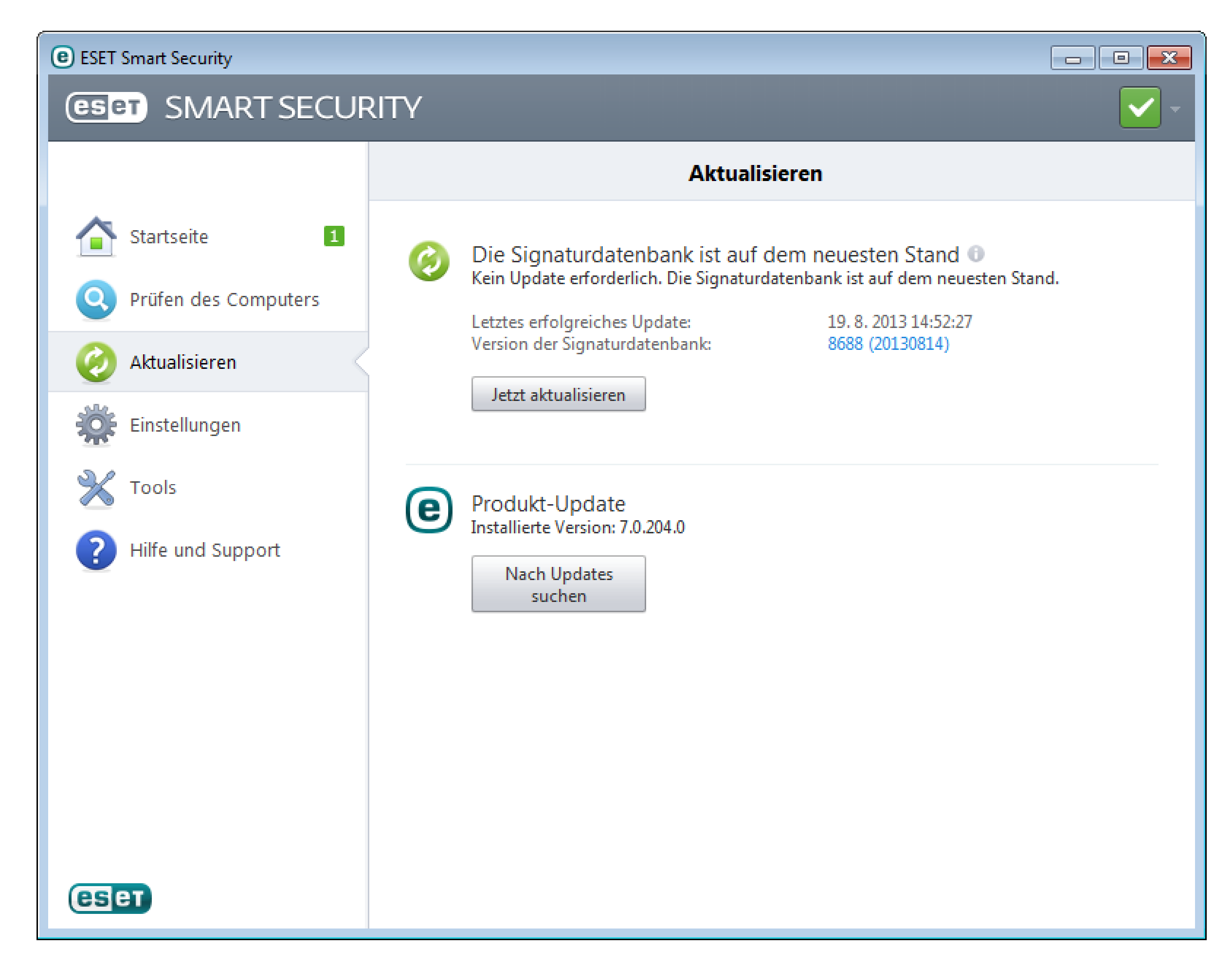
4.5 Aktualisieren des Programms

Den optimalen Schutz Ihres Computers gewährleisten Sie, indem Sie ESET Smart Security regelmäßig aktualisieren. Die Updates halten das Programm fortlaufend auf dem neuesten Stand, indem die Signaturdatenbank und die Programmkomponenten aktualisiert werden.

Über den Punkt **Update** im Hauptprogrammfenster können Sie sich den aktuellen Update-Status anzeigen lassen. Sie sehen hier Datum und Uhrzeit des letzten Updates und können feststellen, ob ein Update erforderlich ist. Die Versionsnummer der Signaturdatenbank wird ebenfalls in diesem Fenster angezeigt. Diese Nummer ist ein aktiver Link zur Website von ESET, auf der alle Signaturen aufgeführt werden, die bei dem entsprechenden Update hinzugefügt wurden.

Zusätzlich zu automatischen Updates können Sie auf **Jetzt aktualisieren** klicken, um ein Update manuell auszulösen. Updates der Signaturdatenbank und Updates von Programmkomponenten sind wichtige Bestandteile der Maßnahmen für einen möglichst umfassenden Schutz vor Schadcode. Seien Sie deshalb bei Konfiguration und Ausführung besonders sorgfältig. Wenn Sie Ihre Lizenzdaten (Benutzername und Passwort) nicht während der Installation eingegeben haben, können Sie sie beim Update eingeben, um auf die ESET-Update-Server zuzugreifen.

HINWEIS: Ihren Benutzernamen und das Passwort erhalten Sie von ESET nach dem Kauf von ESET Smart Security.



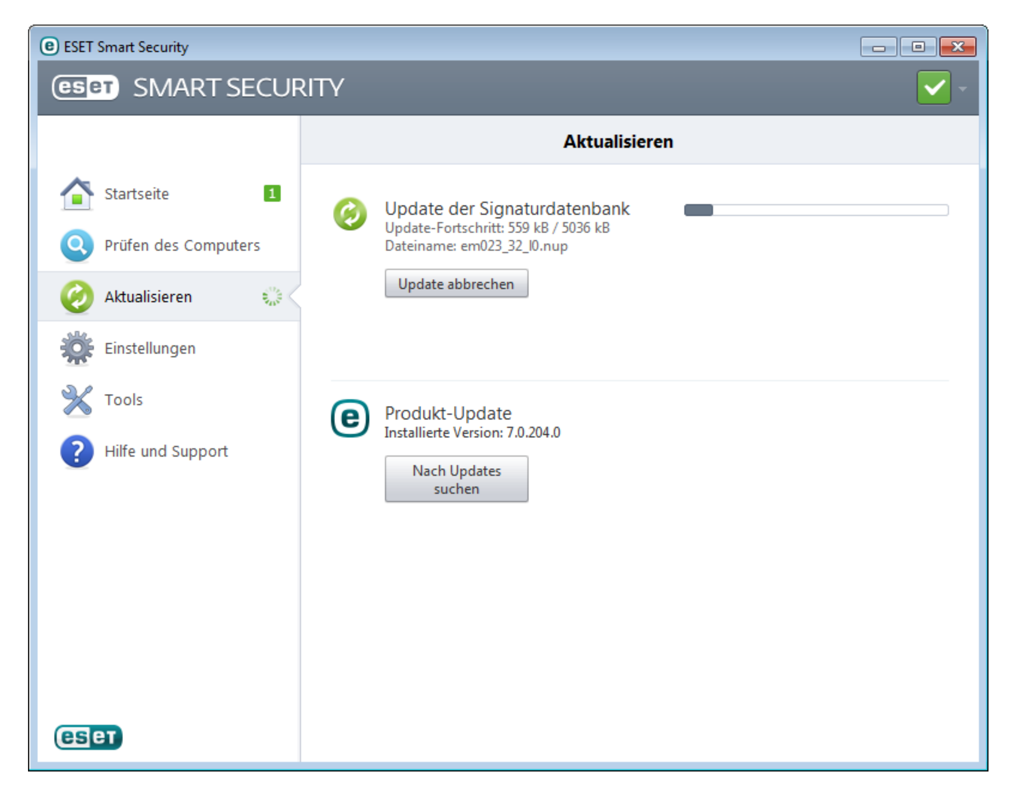
Letztes erfolgreiches Update - Das Datum des letzten Updates. Wenn das angezeigte Datum bereits einige Zeit zurückliegt, ist die Signaturdatenbank möglicherweise nicht auf dem neuesten Stand.

Version der Signaturdatenbank - Die Nummer der Signaturdatenbank. Diese Nummer ist gleichzeitig ein aktiver Link zur Website von ESET. Klicken Sie darauf, um eine Liste aller Signaturen anzuzeigen, die bei dem entsprechenden Update hinzugefügt wurden.

Klicken Sie auf **Nach Updates suchen**, um die neueste verfügbare Version ESET Smart Security zu ermitteln.

Update-Vorgang

Nach einem Klick auf **Jetzt aktualisieren** startet der Download. Eine Fortschrittsanzeige und die verbleibende Zeit wird angezeigt. Um den Update-Vorgang abzubrechen, klicken Sie auf **Update abbrechen**.



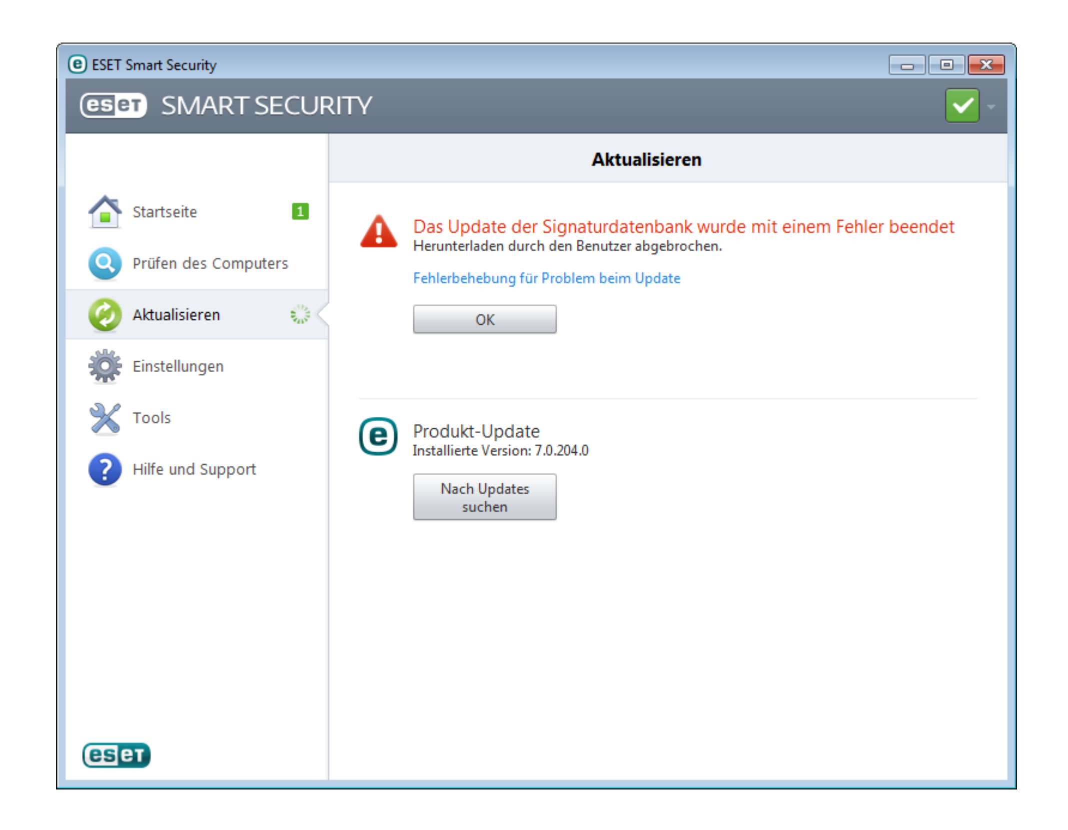
Wichtig: Wenn keinerlei Zwischenfälle beim Update-Download auftreten, wird im **Update**-Fenster der Hinweis **Update nicht erforderlich - die Signaturdatenbank ist auf dem neuesten Stand** angezeigt. Andernfalls ist das Programm nicht auf dem neuesten Stand und anfälliger für Infektionen. Aktualisieren Sie die Signaturdatenbank so schnell wie möglich. In allen anderen Fällen erhalten Sie eine der folgenden Fehlermeldungen:

Signaturdatenbank nicht mehr aktuell - Dieser Fehler wird angezeigt, wenn die Signaturdatenbank trotz wiederholter Versuche nicht aktualisiert werden konnte. Sie sollten in diesem Fall die Update-Einstellungen überprüfen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten oder fehlerhaft konfigurierte Verbindungseinstellungen.

Die eben erwähnte Meldung steht im Zusammenhang mit den folgenden beiden **Während des Updates der Signaturdatenbank sind Fehler aufgetreten**-Meldungen über nicht erfolgreiche Updates:

1. **Benutzername und/oder Passwort falsch** - Der Benutzername und das Passwort wurden unter „Einstellungen für Updates“ falsch eingegeben. Wir empfehlen eine Überprüfung Ihrer Lizenzdaten. Das Fenster „Erweiterte Einstellungen“ (klicken Sie im Hauptmenü auf **Einstellungen** und dann auf **Erweiterte Einstellungen** oder drücken Sie F5 auf Ihrer Tastatur) enthält zusätzliche Update-Optionen. Klicken Sie in der Baumstruktur der erweiterten Einstellungen auf **Update** > **Einstellungen**, um Benutzername und Passwort neu einzugeben.

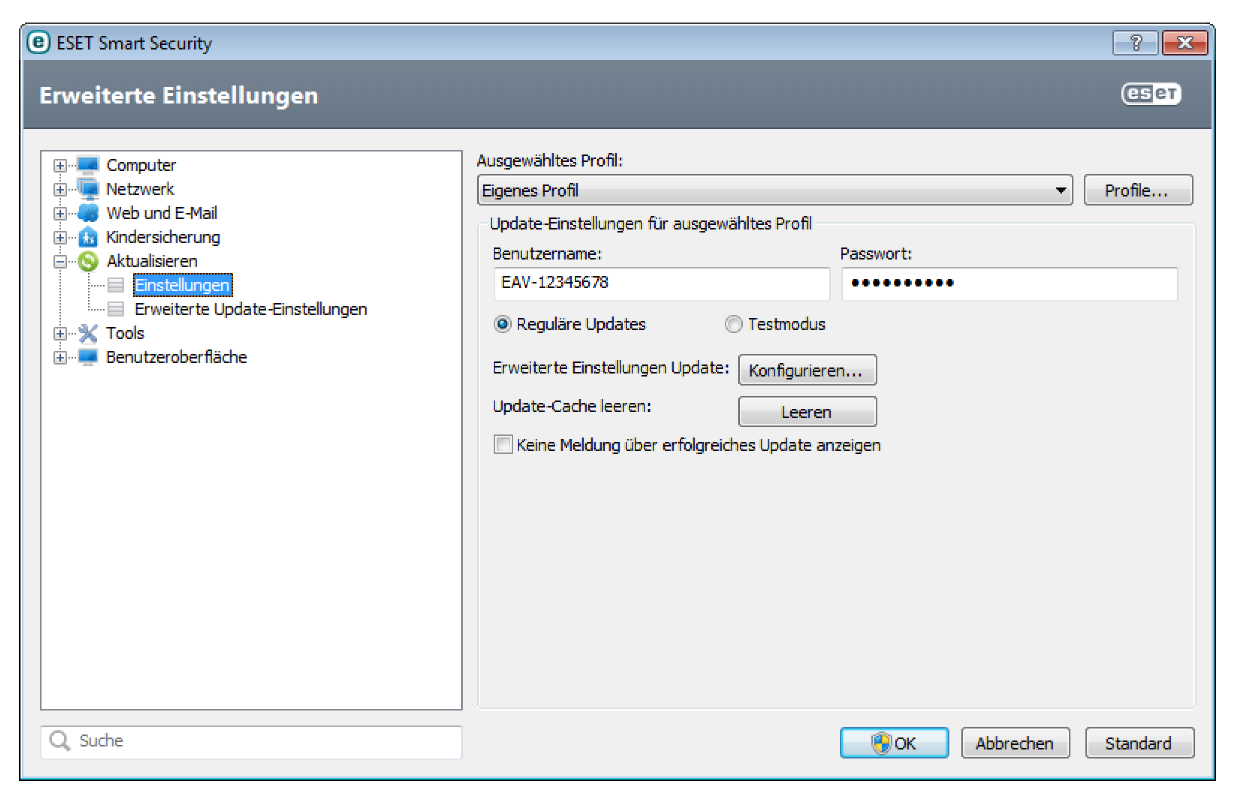
2. **Fehler beim Herunterladen der Update-Dateien** - Ein Grund für den Fehler könnten falsche Einstellungen der Internetverbindung sein. Überprüfen Sie die Internetverbindung, z. B. indem Sie eine beliebige Internetseite im Webbrowser aufrufen. Wenn die Website nicht aufgerufen werden kann, besteht mit ziemlicher Sicherheit keine Internetverbindung. Falls dies der Fall ist, wenden Sie sich an Ihren Internetdienstanbieter.



4.5.1 Update-Einstellungen

Die Optionen für die Update-Einstellungen finden Sie im Fenster **Erweiterte Einstellungen** (Taste F5) unter **Update** > **Update**. In diesem Bereich finden Sie Informationen zum Abruf von Updates, z. B. die Liste der Update-Server und die Anmeldedaten für diese Server. In der Home-Version von ESET-Produkten kann der Update-Server nicht frei gewählt werden. Updates werden automatisch von dem ESET-Server heruntergeladen, der am wenigsten belastet ist. Das Dropdown-Menü **Update-Server** ist nur in ESET Endpoint Antivirus oder ESET Endpoint Security verfügbar.

Die Updates können nur dann ordnungsgemäß heruntergeladen werden, wenn alle Update-Informationen richtig eingegeben wurden. Falls Sie eine Firewall verwenden, stellen Sie sicher, dass das Programm Verbindungen mit dem Internet herstellen darf (HTTP-Kommunikation ist aktiviert).



Ihr aktuelles Update-Profil wird im Dropdown-Menü **Ausgewähltes Profil** angezeigt. Klicken Sie auf **Profile**, um ein neues Profil zu erstellen.

Zur Anmeldung beim Update-Server verwenden Sie den **Benutzernamen** und das **Passwort**, die beim Kauf erzeugt und Ihnen zugestellt wurden. Standardmäßig wird keine Anmeldung verlangt und die Felder **Benutzername** und **Passwort** bleiben leer.

Der Testmodus (Option **Testmodus**) stellt Updates bereit, die intern umfangreich geprüft wurden und in absehbarer Zeit allgemein verfügbar sein werden. Wenn Sie den Testmodus aktivieren, können Sie früher von den neuesten Erkennungsmethoden und Fehlerkorrekturen profitieren. Da jedoch letzte Fehler nicht ausgeschlossen werden können, sind diese Updates ausdrücklich NICHT für Rechner im Produktivbetrieb vorgesehen, die durchgängig stabil und verfügbar laufen müssen. Unter **Hilfe und Support** > **Über ESET Smart Security** können Sie die Liste der aktuellen Module einsehen. Es wird empfohlen, die Option **Reguläre Updates** aktiviert zu lassen (Standard).

Klicken Sie zum Anzeigen der erweiterten Update-Einstellungen auf **Einstellungen...** neben **Erweiterte Einstellungen für Updates**.

Wenn Probleme mit einem Update auftreten, klicken Sie auf **Leeren...**, um temporäre Update-Dateien zu löschen.

Keine Meldung über erfolgreiches Update anzeigen - Deaktiviert die Hinweise im Infobereich der Taskleiste rechts unten auf dem Bildschirm. Diese Option ist sinnvoll, wenn eine Anwendung im Vollbildmodus oder ein Spiel ausgeführt wird. Beachten Sie, dass die Anzeige von Meldungen im Gamer-Modus deaktiviert ist.

4.5.1.1 Update-Profile

Update-Profile können für verschiedene Update-Konfigurationen und -Tasks erstellt werden. Besonders sinnvoll ist das Erstellen von Update-Profilen für mobile Benutzer, die auf regelmäßige Änderungen bei der Internetverbindung mit entsprechenden Profilen reagieren können.

Die Liste **Ausgewähltes Profil** zeigt das aktuelle Profil an; standardmäßig ist dies **Mein Profil**. Zum Erstellen eines neuen Profils klicken Sie auf **Profile** und dann auf **Hinzufügen**. Geben Sie anschließend den **Namen des Profils** ein. Wenn Sie ein neues Profil erstellen, können Sie die Einstellungen eines bereits bestehenden Profils kopieren, indem Sie die Option **Einstellungen kopieren von Profil** aus der Liste wählen.

Im Fenster mit den Profileinstellungen können Sie den Update-Server in einer Liste verfügbarer Server angeben oder einen neuen Server hinzufügen. Das Dropdown-Menü **Update-Server** zeigt eine Aufstellung der vorhandenen Update-Server. Um einen neuen Update-Server hinzuzufügen, klicken Sie im Bereich **Update-Einstellungen für ausgewähltes Profil** auf **Bearbeiten**. Klicken Sie anschließend auf **Hinzufügen**.

4.5.1.2 Erweiterte Einstellungen für Updates

Klicken Sie zum Anzeigen der erweiterten Einstellungen für Updates auf **Einstellungen**. In den erweiterten Einstellungen finden Sie Optionen zur Konfiguration von **Update-Modus**, **HTTP-Proxy** und **LAN**.

4.5.1.2.1 Update-Modus

Auf der Registerkarte **Update-Modus** finden Sie Optionen zum Aktualisieren der Programmkomponenten. Sie können festlegen, wie das Programm reagieren soll, wenn neue Updates für Programmkomponenten verfügbar sind.

Mit Updates für Programmkomponenten (PCUs) können neue Funktionen in das Programm integriert oder Funktionen aus früheren Versionen modifiziert werden. Updates für Programmkomponenten können automatisch oder einzeln nach Bestätigung durch den Benutzer gestartet werden. Nach der Installation von Updates der Programmkomponenten muss der Computer möglicherweise neu gestartet werden. Im Abschnitt **Updates für Programmkomponenten** stehen drei Optionen zur Verfügung:

- **Niemals ausführen** - Es werden keine Updates für Programmkomponenten ausgeführt. Diese Option wird für Server empfohlen, da Server normalerweise nur im Rahmen geplanter Wartungsarbeiten neu gestartet werden dürfen.
- **Immer ausführen** - Updates zu Programmkomponenten werden heruntergeladen und automatisch installiert. Beachten Sie, dass nach der Installation von Programmkomponenten möglicherweise der Computer neu gestartet werden muss.
- **Benutzer fragen** - Dies ist die Standardoption. Stehen Updates für Programmkomponenten zur Verfügung, werden Sie aufgefordert, sie zu bestätigen oder abzulehnen.

Nach der Installation eines Updates für Programmkomponenten kann ein Neustart Ihres Computers erforderlich werden, um die Funktionalität aller Module zu gewährleisten. Im Bereich **Computerneustart, falls nach Upgrade erforderlich** kann der Benutzer eine der folgenden drei Optionen auswählen:

- **Niemals ausführen** - Es erfolgt keine Aufforderung zum Neustarten des Computers, unabhängig davon, ob ein Neustart erforderlich ist oder nicht. Es wird nicht empfohlen, diese Option zu aktivieren, da die Funktion des Computers bis zum Neustart eingeschränkt sein kann.
- **Benutzer fragen** - Dies ist die Standardoption. Falls nach der Installation von Updates für Programmkomponenten ein Neustart des Computers erforderlich ist, werden Sie zur Bestätigung aufgefordert.
- **Automatisch OHNE Benutzerbestätigung (Vorsicht auf Servern)** - Falls nach der Installation von Updates für Programmkomponenten ein Neustart des Computers erforderlich ist, wird der Computer ohne Nachfrage neu gestartet.

HINWEIS: Die Auswahl der geeigneten Option hängt vom jeweiligen Computer ab, auf dem die Einstellungen ausgeführt werden. Beachten Sie die unterschiedliche Funktion von Arbeitsplatzcomputern und Servern. Das automatische Neustarten eines Servers nach einem Update kann schwerwiegende Folgen haben.

Wenn die Option **Vor dem Herunterladen von Updates fragen** aktiviert ist, wird ein Hinweis angezeigt, wenn ein neues Update verfügbar ist.

Übersteigt die Größe des Updates den unter **Fragen, falls Update größer ist als** angegebene Wert, wird ein Hinweis angezeigt.

Die Option **Regelmäßig nach aktueller Produktversion suchen** aktiviert den Task **Regelmäßige Überprüfung auf aktuelle Produktversion** (siehe Taskplaner).

4.5.1.2.2 Proxyserver

Zu den Optionen für Proxyserver-Einstellungen gelangen Sie über **Update** in den erweiterten Einstellungen (F5). Klicken Sie dann auf **Einstellungen** rechts neben **Erweiterte Einstellungen für Updates**. Klicken Sie auf die Registerkarte **HTTP-Proxy** und wählen Sie eine dieser drei Optionen:

- **In Systemsteuerung eingestellten Proxy verwenden**
- **Keinen Proxyserver verwenden**
- **Verbindung über Proxyserver**

Mit dem Aktivieren der Option **In Systemsteuerung eingestellten Proxy verwenden** wird die unter „Erweiterte Einstellungen“ (**Tools** > **Proxyserver**) bereits festgelegte Proxyserver-Konfiguration übernommen.

Mit der Option **Keinen Proxyserver verwenden** legen Sie fest, dass kein Proxyserver für Updates von ESET Smart Security genutzt wird.

Die Option **Verbindung über Proxyserver** sollten Sie wählen, wenn:

- Ein Proxyserver für Updates von ESET Smart Security benötigt wird, bei dem es sich nicht um den in den allgemeinen Einstellungen festgelegten Proxyserver handelt (**Tools** > **Proxyserver**). In diesem Fall sind an dieser Stelle Einstellungen erforderlich: **Proxyserver**-Adresse, **Port** sowie **Benutzername** und **Passwort** für den Proxyserver, falls erforderlich.
- Die Proxyserver-Einstellungen nicht für das gesamte Programm festgelegt wurden, ESET Smart Security jedoch Updates über einen Proxyserver herunterladen soll.
- Ihr Computer über einen Proxyserver mit dem Internet verbunden ist. Während der Installation werden die Einstellungen aus Internet Explorer übernommen. Falls Sie später Änderungen vornehmen (zum Beispiel wenn Sie den Internetanbieter wechseln), müssen Sie hier die HTTP-Proxy-Einstellungen prüfen und gegebenenfalls ändern. Sonst kann keine Verbindung zu den Update-Servern hergestellt werden.

Die Standardeinstellung für den Proxyserver ist **In Systemsteuerung eingestellten Proxy verwenden**.

HINWEIS: Die Felder mit den Anmeldedaten (**Benutzername** und **Passwort**) sind nur für den Zugriff auf den Proxyserver vorgesehen. Geben Sie in diesen Feldern nur Daten ein, wenn diese für den Zugriff auf den Proxyserver erforderlich sind. Beachten Sie, dass in diese Felder nicht das Passwort und der Benutzername für ESET Smart Security eingetragen werden. Eine Eingabe ist nur dann erforderlich, wenn Sie für die Internetverbindung über den Proxyserver ein Passwort benötigen.

4.5.1.2.3 Herstellen einer LAN-Verbindung

Beim Aktualisieren von einem lokalen Server mit einem Betriebssystem auf Windows NT-Basis ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich.

Zum Konfigurieren eines solchen Kontos klicken Sie auf die Registerkarte **LAN**. Der Bereich **Verbindung mit dem LAN herstellen als** enthält die Optionen **Systemkonto (Standard)**, **Aktueller Benutzer** und **Folgender Benutzer**.

Wählen Sie **Systemkonto (Standard)**, um das Systemkonto für die Authentifizierung zu verwenden. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Anmeldedaten angegeben sind.

Wenn sich das Programm mit dem Konto des aktuell angemeldeten Benutzers anmelden soll, wählen Sie **Aktueller Benutzer**. Nachteil dieser Option ist, dass das Programm keine Verbindung zum Update-Server herstellen kann, wenn kein Benutzer angemeldet ist.

Wählen Sie **Folgender Benutzer**, wenn das Programm ein spezielles Benutzerkonto für die Authentifizierung verwenden soll. Nutzen Sie diese Option, wenn eine Anmeldung mit dem standardmäßigen Systemkonto nicht möglich ist. Beachten Sie, dass für das ausgewählte Benutzerkonto Zugriffsrechte auf den Ordner mit den Update-Dateien definiert sein müssen. Wenn keine Zugriffsrechte definiert sind, kann das Programm keine Updates abrufen.

Warnung: Wenn entweder **Aktueller Benutzer** oder **Folgender Benutzer** aktiviert ist, kann ein Fehler beim Wechsel der Identität zum gewünschten Benutzer auftreten. Aus diesem Grund wird empfohlen, die LAN-Anmeldedaten in den Haupteinstellungen für Updates einzugeben. In diesen Update-Einstellungen geben Sie die Anmeldedaten wie folgt ein: *Domänenname\Benutzer* (bei einer Arbeitsgruppe geben Sie *Arbeitsgruppenname\Name* ein) und das Passwort. Bei Aktualisierung von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

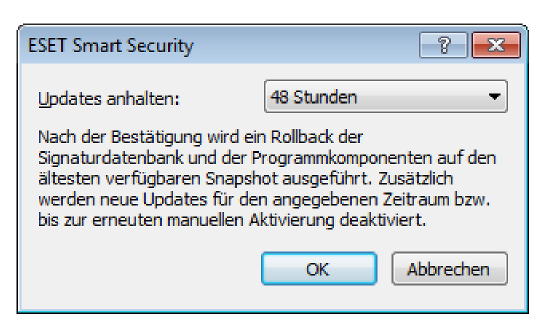
Aktivieren Sie die Option **Nach Update Verbindung zum Server trennen**, wenn die Verbindung zum Server nach dem Abrufen von Update-Dateien aktiv bleibt.

4.5.2 Update-Rollback

Wenn Sie befürchten, dass ein neues Update der Signaturdatenbank oder eines Programmmoduls korrupt oder nicht stabil ist, können Sie einen Rollback zur vorigen Version ausführen und Updates für einen bestimmten Zeitraum deaktivieren. Hier können Sie auch zuvor für einen unbegrenzten Zeitraum deaktivierte Updates wieder aktivieren.

ESET Smart Security zeichnet Snapshots der Signaturdatenbank und der Programmmodule zur späteren Verwendung mit der *Rollback*-Funktion auf. Um Snapshots der Signaturdatenbank zu erstellen, lassen Sie das Kontrollkästchen **Snapshots der Update-Dateien erstellen** aktiviert. Das Feld **Zahl der lokal gespeicherten Snapshots** legt fest, wie viele vorige Snapshots der Signaturdatenbank gespeichert werden.

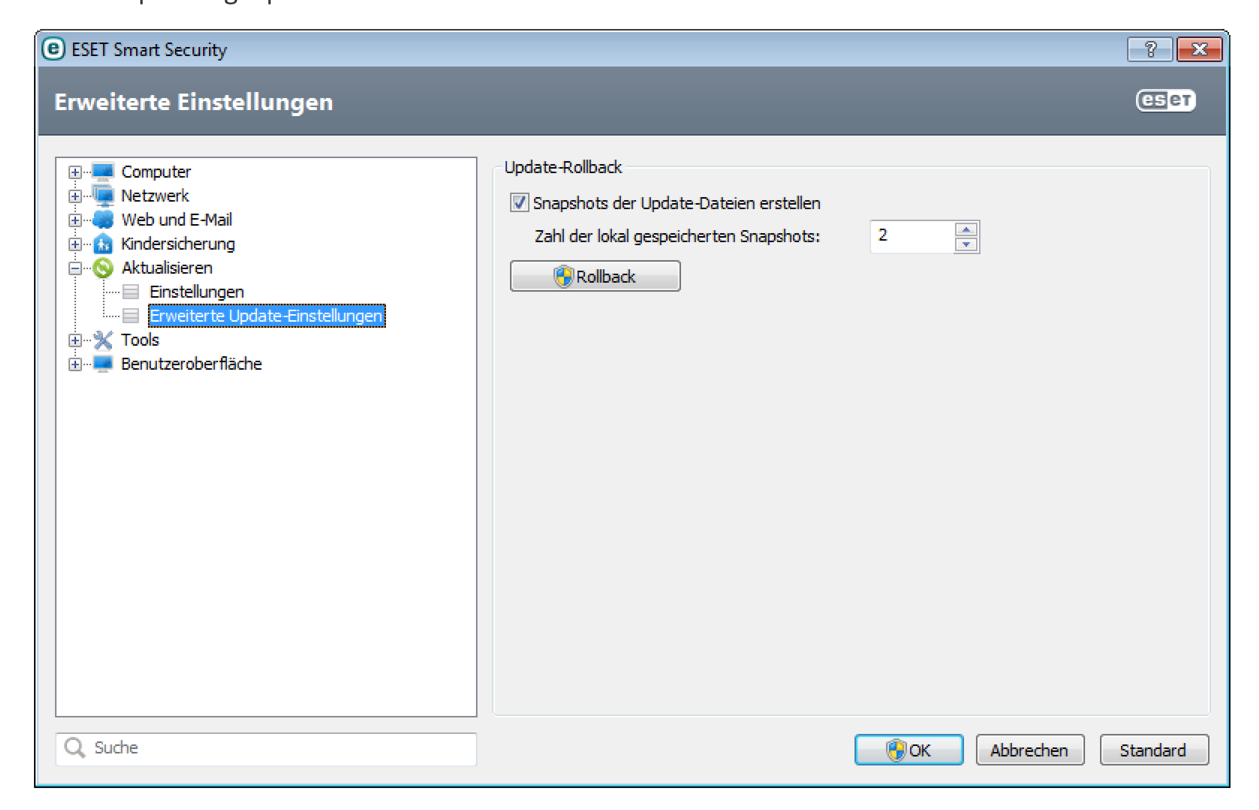
Wenn Sie auf **Rollback ausführen** (**Erweiterte Einstellungen** (F5) > **Update** > **Erweitert**) klicken, müssen Sie im Dropdown-Menü **Updates unterbrechen** einen Zeitraum auswählen. Dieser Wert legt fest, wie lange die Updates der Signaturdatenbank und der Programmkomponenten ausgesetzt werden.



Wählen Sie **bis zum Widerrufen**, um keine regelmäßigen Updates auszuführen, bis die Update-Funktion manuell wieder aktiviert wird. Das Aktivieren dieser Option ist mit einem Sicherheitsrisiko verbunden und daher nicht empfehlenswert.

Wenn ein Rollback durchgeführt wird, wechselt die Schaltfläche **Rollback** zu **Updates erlauben**. Für die im

Dropdown-Menü **Updates anhalten** angegebene Dauer werden keine Updates zugelassen. Die Version der Signaturdatenbank wird auf die älteste verfügbare Version herabgestuft und als Snapshot im lokalen Dateisystem des Computers gespeichert.



Beispiel: Die aktuellste Version der Signaturdatenbank ist beispielsweise 6871. Die Versionen 6870 und 6868 sind als Snapshots der Signaturdatenbank gespeichert. Die Version 6869 ist nicht verfügbar, weil der Computer beispielsweise eine Zeit lang heruntergefahren war und ein aktuelleres Update verfügbar war, bevor Version 6869 heruntergeladen wurde. Wenn Sie in das Feld **Zahl der lokal gespeicherten Snapshots** den Wert „2“ (zwei) eingegeben haben und auf **Rollback ausführen** klicken, wird die Version 6868 der Signaturdatenbank (und Programmmodule) wiederhergestellt. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Überprüfen Sie, ob die Version der Signaturdatenbank im Hauptprogrammfenster von ESET Smart Security im Abschnitt Update herabgestuft wurde.

4.5.3 So erstellen Sie Update-Tasks

Mit der Option **Signaturdatenbank aktualisieren** können Updates manuell ausgeführt werden. Klicken Sie dazu im Hauptmenü auf **Update** und wählen Sie im daraufhin angezeigten Dialogfenster die entsprechende Option aus.

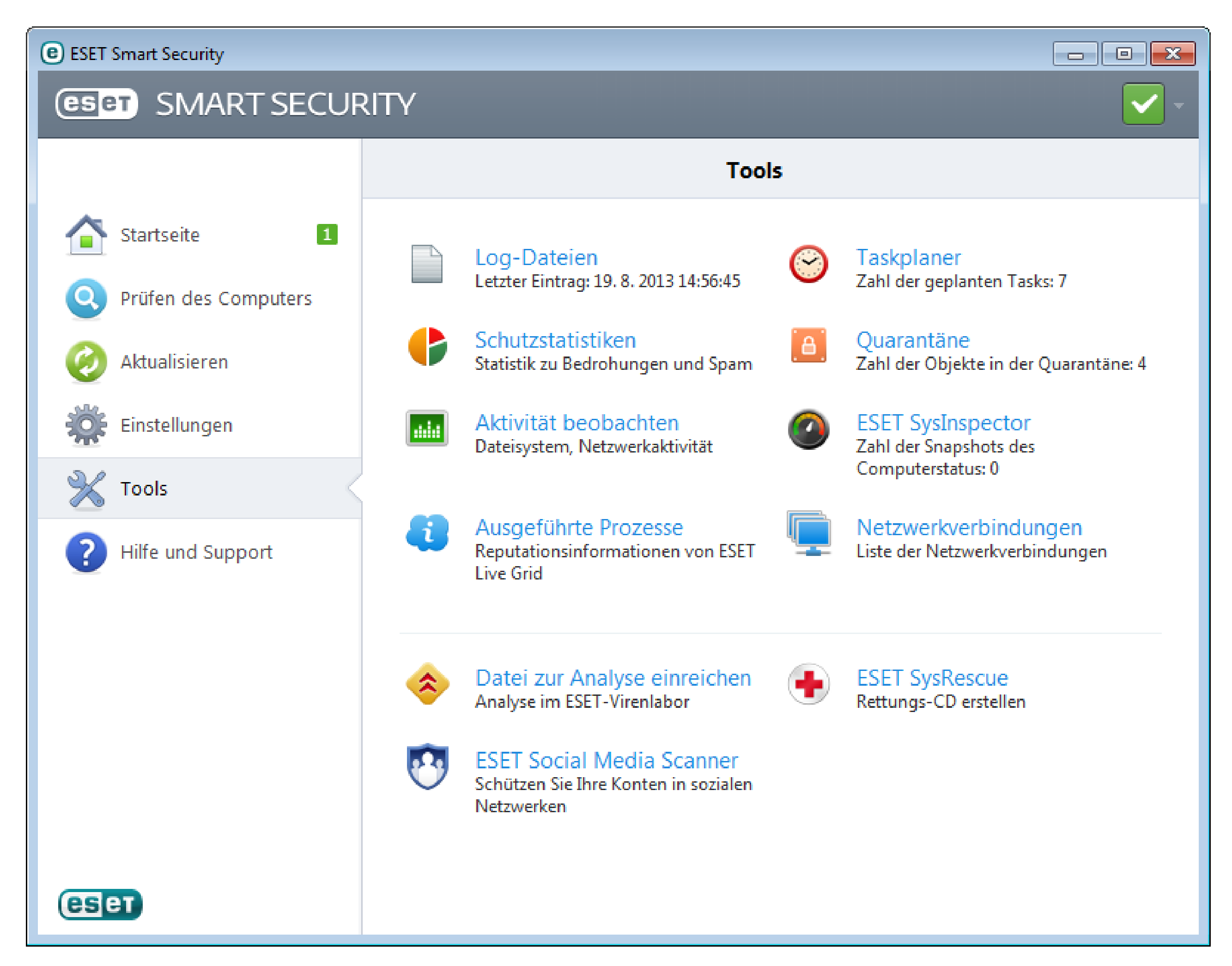
Darüber hinaus können Sie Updates auch als geplante Tasks einrichten. Um einen Task zu konfigurieren, klicken Sie auf **Tools** > **Taskplaner**. Standardmäßig sind in ESET Smart Security folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**

Jeder Update-Task kann bei Bedarf angepasst werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie im Abschnitt Taskplaner.

4.6 Tools

Das Menü **Tools** enthält Module, die die Verwaltung des Programms vereinfachen und zusätzliche Optionen für erfahrene Benutzer bereitstellen.



Dieser Bereich enthält die folgenden Elemente:

- Log-Dateien
- Schutzstatistiken
- Aktivität beobachten
- Ausgeführte Prozesse (wenn ESET Live Grid in ESET Smart Security aktiviert ist)
- Taskplaner
- Quarantäne
- Netzwerkverbindungen (wenn Personal Firewall in in ESET Smart Security integriert ist)
- ESET SysInspector

Datei zur Analyse einreichen - Ermöglicht Ihnen, eine verdächtige Datei zur Analyse bei ESET einzureichen. Das Dialogfenster, das nach dem Anklicken dieser Option erscheint, wird unter Dateien zur Analyse einreichen beschrieben.

ESET SysRescue - Startet den ESET SysRescue-Installationsassistenten.

Hinweis: ESET SysRescue in ESET Smart Security 6 ist momentan nicht für Windows 8 verfügbar. Sie sollten daher ein Produkt-Upgrade durchführen oder einen ESET SysRescue-Datenträger unter einer anderen Version von Microsoft Windows erstellen.

ESET Social Media Scanner – Link zu einer Anwendung in sozialen Medien (z. B. Facebook), die Benutzer sozialer Medien vor Bedrohungen schützt. Die Anwendung ist unabhängig von anderen ESET-Produkten und kostenlos.

4.6.1 Log-Dateien

Die Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Das Erstellen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Bedrohungen sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus ESET Smart Security heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.

Log-Dateien können über das Hauptprogrammfenster aufgerufen werden, indem Sie auf **Tools** > **Log-Dateien** klicken. Wählen Sie im Dropdown-Menü **Log** den gewünschten Log-Typ aus. Folgende Logs sind verfügbar:

- **Erkannte Bedrohungen** - Das Bedrohungs-Log enthält detaillierte Informationen über eingedrungene Schadsoftware, die von ESET Smart Security entdeckt wurde. Zu den Informationen gehören die Zeit der Erkennung, der Name der eingedrungenen Schadsoftware, der Ort, an dem sie sich befindet, die ausgeführten Aktionen und der Name des Benutzers, der zur Zeit der Entdeckung der eingedrungenen Schadsoftware angemeldet war. Doppelklicken Sie auf einen Log-Eintrag, um die Details in einem eigenen Fenster anzuzeigen.

- **Ereignisse** - Alle von ESET Smart Security ausgeführten wichtigen Aktionen werden im Ereignis-Log aufgezeichnet. Das Ereignis-Log enthält Informationen über Ereignisse und im Programm aufgetretene Fehler. Es unterstützt Systemadministratoren und Benutzer bei der Fehlerbehebung. Die hier aufgeführten Informationen sind oftmals hilfreich, um ein im Programm aufgetretenes Problem zu beheben.

- **Computer prüfen** - In diesem Fenster werden die Ergebnisse aller manuell durchgeführten oder geplanten Prüfungen angezeigt. Jede Zeile entspricht der Überprüfung eines einzelnen Computers. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu der entsprechenden Prüfung anzeigen.

- **HIPS** - Enthält Einträge spezifischer HIPS-Regeln, die zum Aufzeichnen markiert wurden. Das Protokoll zeigt die Anwendung an, die den Vorgang ausgelöst hat, das Ergebnis (ob der Vorgang zugelassen oder blockiert wurde) sowie den erstellten Regelnamen.

- **Personal Firewall** - Das Firewall-Log zeigt alle von der Personal Firewall entdeckten Angriffe von anderen Computern an. Hier erhalten Sie Informationen über alle Angriffe auf Ihren Computer. In der Spalte *Ereignis* werden die entdeckten Angriffe angezeigt. Unter *Quelle* erfahren Sie mehr über den Angreifer. Die Spalte *Protokoll* zeigt das für den Angriff verwendete Datenübertragungsprotokoll an. Eine Analyse des Firewall-Logs hilft Ihnen dabei, Eindringversuche von Schadsoftware rechtzeitig zu erkennen, um den unerlaubten Zugriff auf Ihr System zu verhindern.

- **Gefilterte Websites** - Diese Liste enthält die durch den Web-Schutz oder die Kindersicherung gesperrten Websites. Die Logs enthalten die Uhrzeit, die URL-Adresse, den Benutzer und die Anwendung, die eine Verbindung zur gegebenen Website erstellt hat.

- **Spam-Schutz** - Enthält Einträge zu E-Mails, die als Spam eingestuft wurden.

- **Kindersicherung** - Zeigt die Webseiten an, die über die Kindersicherung zugelassen bzw. gesperrt wurden. Die Spalten *Übereinstimmungstyp* und *Übereinstimmungswerte* geben an, wie die Filterregeln angewendet wurden.

- **Medienkontrolle** - Enthält Datensätze zu Wechselmedien oder externen Geräten, die an den Computer angeschlossen wurden. Nur Geräte mit einer entsprechenden Regel für die Medienkontrolle werden in die Log-Datei aufgenommen. Wenn auf ein angeschlossenes Gerät keine Regel zutrifft, wird für das Gerät kein Log-Eintrag erstellt. Hier können Sie außerdem Details wie Gerätetyp, Seriennummer, Herstellername und Mediengröße (je nach Verfügbarkeit der Informationen) anzeigen.

In jedem Abschnitt können die angezeigten Informationen direkt in die Zwischenablage kopiert werden (Tastaturbefehl Strg+C). Wählen Sie dazu die gewünschten Einträge aus und klicken Sie auf **Kopieren**. Zur Auswahl mehrerer Einträge verwenden Sie die Strg- und die Umschalttaste.

Das Kontextmenü können Sie über einen Rechtsklick auf einen Eintrag öffnen. Im Kontextmenü stehen folgende Optionen zur Verfügung:

- **Einträge desselben Typs filtern** - Wenn Sie diesen Filter aktivieren, werden nur Einträge desselben Typs angezeigt (Diagnose, Warnungen, ...).
- **Filter/Suchen**- Wenn diese Option aktiviert ist, wird das Fenster **Log-Filter** angezeigt, in dem Sie die Filterkriterien festlegen können.
- **Filter deaktivieren** - Setzt alle Filtereinstellungen (wie oben beschrieben) zurück
- **Alles kopieren** - Kopiert die Informationen zu allen im Fenster angezeigten Einträgen
- **Löschen/Alle löschen** - Löscht die ausgewählten oder alle angezeigten Einträge; für diese Option sind Administratorrechte erforderlich
- **Exportieren** - Exportiert Informationen zu den Einträgen im XML-Format
- **Ähnliche Ereignisse zukünftig nicht blockieren** - Diese Option ist nur im Firewall-Log sichtbar. Fügt eine IDS-Ausnahme für die ausgewählte Aktivität zur Personal Firewall hinzu.
- **Bildlauf für Log** - Wenn diese Option aktiv ist, wandern alte Logs automatisch aus der Anzeige, sodass im Fenster **Log-Dateien** die neuesten Einträge sichtbar sind.

4.6.1.1 Log-Wartung

Die Log-Konfiguration für ESET Smart Security können Sie aus dem Hauptprogrammfenster aufrufen. Klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Tools** > **Log-Dateien**. In diesem Bereich können Sie Einstellungen für Logs festlegen. Um den Speicherbedarf zu reduzieren, werden ältere Logs automatisch gelöscht. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

Mindestinformation in Logs - Hier können Sie festlegen, welche Ereignistypen in Logs aufgezeichnet werden sollen.

- **Diagnose** - Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen** - Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** - Kritische Fehler und Warnungen werden protokolliert.
- **Fehler** - Fehler wie *„Fehler beim Herunterladen der Datei“* und kritische Fehler werden aufgezeichnet.
- **Kritische Warnungen** - Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls, beim Ausführen der Personal Firewallusw.) werden protokolliert.

Log-Einträge, die älter sind als die unter **Einträge automatisch löschen nach (Tage)** angegebene Anzahl an Tagen, werden automatisch gelöscht.

Log-Dateien automatisch optimieren - Ist diese Option aktiviert, werden die Log-Dateien automatisch defragmentiert, wenn die Prozentzahl höher ist als der unter **wenn ungenutzte Einträge größer als (%)** angegebene Wert.

Klicken Sie zum Defragmentieren der Log-Dateien auf **Jetzt optimieren**. Um die Systemleistung und -geschwindigkeit beim Verarbeiten der Log-Dateien zu erhöhen, werden alle leeren Log-Einträge entfernt. Eine starke Verbesserung ist insbesondere dann erkennbar, wenn die Logs eine große Anzahl an Einträgen enthalten.

4.6.2 Taskplaner

Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften.

Um ihn zu öffnen, klicken Sie im Hauptprogrammfenster von ESET Smart Security unter **Tools** auf **Taskplaner**. Der **Taskplaner** umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Prüfprofils.

Er dient zur Planung der folgenden Vorgänge: Update der Signaturdatenbank, Prüftask, Prüfung Systemstartdateien und Log-Wartung. Tasks können direkt über das Fenster „Taskplaner“ hinzugefügt oder gelöscht werden. (Klicken Sie dazu unten auf **Hinzufügen** oder **Löschen**.) Klicken Sie an einer beliebigen Stelle mit der rechten Maustaste in das Fenster „Taskplaner“, um folgende Aktionen auszuführen: Anzeigen ausführlicher Informationen, sofortige Ausführung des Vorgangs, Hinzufügen eines neuen Vorgangs und Löschen eines vorhandenen Vorgangs. Verwenden Sie die Kontrollkästchen vor den einzelnen Einträgen zum Aktivieren oder Deaktivieren der jeweiligen Vorgänge.

Standardmäßig werden im **Taskplaner** die folgenden Tasks angezeigt:

- **Log-Wartung**
- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**
- **Regelmäßige Überprüfung auf aktuelle Produktversion** (siehe Update-Modus)
- **Prüfung Systemstartdateien** (nach Benutzeranmeldung)
- **Prüfung Systemstartdateien** (nach Update der Signaturdatenbank)
- **Automatische Erstprüfung**

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, klicken Sie mit der rechten Maustaste auf den Task und dann auf **Bearbeiten**, oder wählen Sie den Task aus, den Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

Hinzufügen eines neuen Tasks

1. Klicken Sie am unteren Fensterrand auf **Hinzufügen**.

2. Wählen Sie dann den gewünschten Task aus der Liste.

3. Geben Sie einen Namen für den Task ein und wählen Sie eine Zeitangabe aus:

   - **Einmalig** - Der Task wird nur einmalig zu einem festgelegten Zeitpunkt ausgeführt.
   - **Wiederholt** - Der Task wird in den (in Stunden) angegebenen Zeitabständen ausgeführt.
   - **Täglich** - Der Task wird täglich zur festgelegten Uhrzeit ausgeführt.
   - **Wöchentlich** - Der Task wird an einem oder mehreren Wochentagen zur festgelegten Uhrzeit ausgeführt.
   - **Bei Ereignis** - Der Task wird ausgeführt, wenn ein bestimmtes Ereignis eintritt.

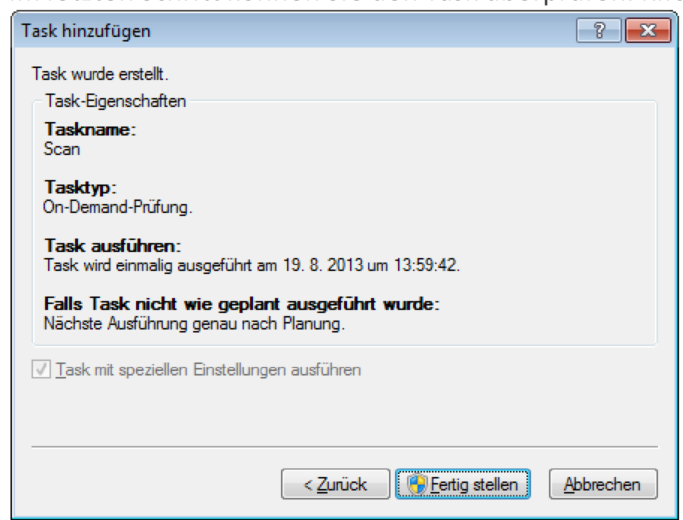
4. Je nach gewählter Zeitangabe wird eines der folgenden Dialogfenster angezeigt:

   - **Einmalig** - Der Task wird nur einmalig zu einem festgelegten Zeitpunkt ausgeführt.
   - **Wiederholt** - Der Task wird in dem angegebenen Zeitabstand ausgeführt.
   - **Täglich** - Der Task wird wiederholt täglich zur festgelegten Uhrzeit ausgeführt.
   - **Wöchentlich** - Der Task wird am festgelegten Wochentag zur angegebenen Uhrzeit ausgeführt.

5. Wenn der Vorgang nicht zur festgelegten Zeit ausgeführt werden konnte, können Sie einen Zeitpunkt für die nächste Ausführung angeben:

   - Nächste Ausführung genau nach Planung
   - Ausführung zum nächstmöglichen Zeitpunkt
   - Sofort ausführen, wenn Zeit seit letzter Ausführung -- Stunden überschreitet

6. Im letzten Schritt können Sie den Task überprüfen. Klicken Sie auf **Fertig stellen**, um den Task zu übernehmen.



4.6.3 Schutzstatistiken

Um statistische Daten zu den Schutzmodulen von ESET Smart Security in einem Diagramm anzeigen zu lassen, klicken Sie auf **Tools** > **Schutzstatistiken**. Wählen Sie im Dropdown-Menü **Statistik** das gewünschte Schutzmodul, um das entsprechende Diagramm und die Legende zu betrachten. Wenn Sie mit dem Mauszeiger über einen bestimmten Punkt in der Legende fahren, werden im Diagramm nur die Daten für diesen Punkt angezeigt.

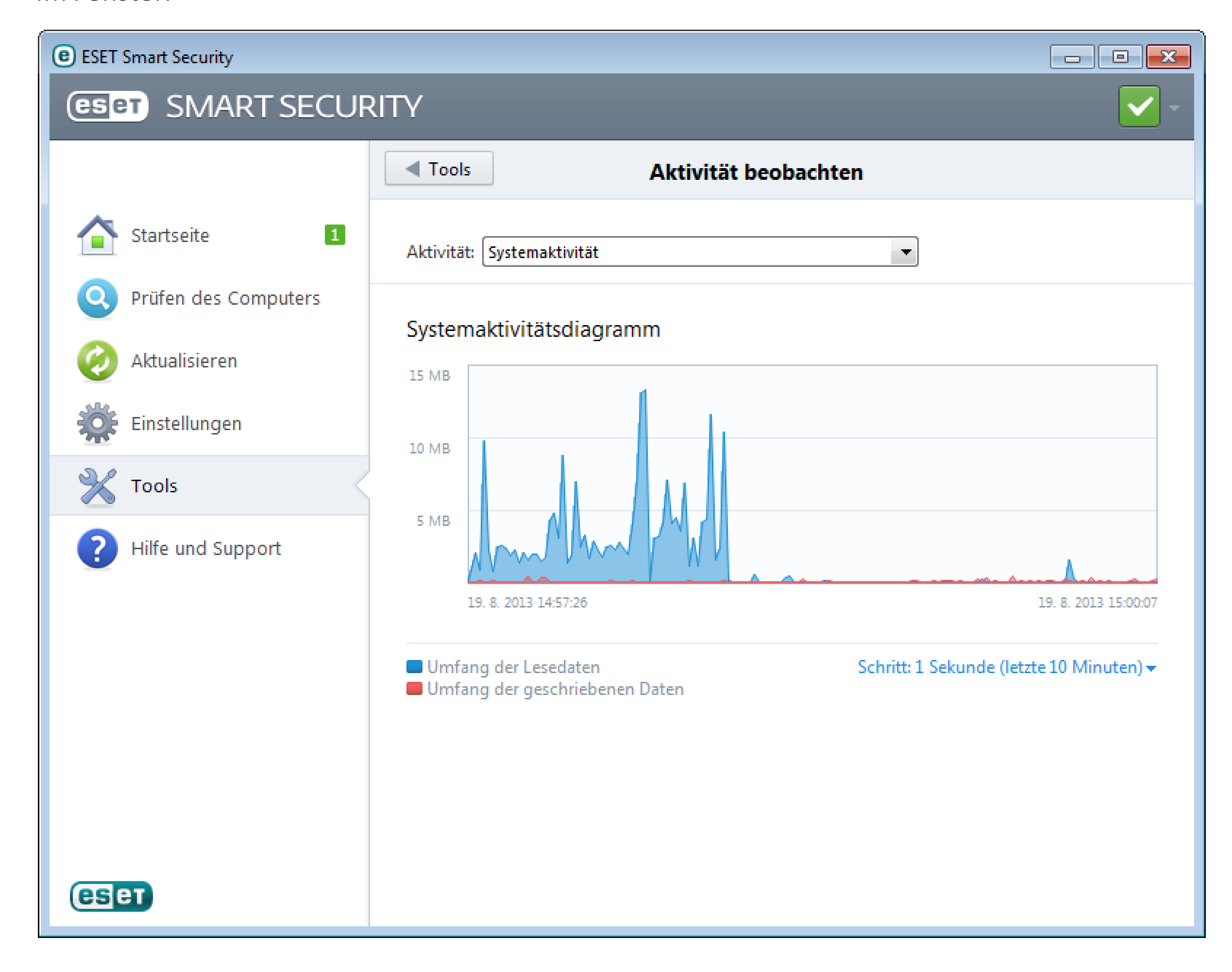
Folgende Diagramme stehen zur Auswahl:

- **Viren- und Spyware-Schutz** - Anzeige der Anzahl infizierter Objekte und gesäuberter Objekte
- **Dateischutz** - Lediglich Anzeige von Objekten, die aus dem Dateisystem gelesen oder in das Dateisystem geschrieben wurden
- **E-Mail-Client-Schutz** - Lediglich Anzeige von Objekten, die von E-Mail-Programmen gesendet oder empfangen wurden
- **Web- und Phishing-Schutz** - Lediglich Anzeige von Objekten, die von einem Webbrowser heruntergeladen wurden
- **E-Mail-Spam-Schutz** - Anzeige der Spam-Schutz-Statistiken seit dem letzten Systemstart

Unter dem Statistik-Diagramm wird die Gesamtanzahl der geprüften Objekte, das zuletzt geprüfte Objekt und der Zeitstempel der Statistik angezeigt. Klicken Sie auf **Zurücksetzen**, um alle Statistikdaten zurückzusetzen.

4.6.4 Aktivität beobachten

Um die aktuelle **Systemaktivität** als Diagramm anzuzeigen, klicken Sie auf **Tools** > **Aktivität beobachten**. Im unteren Bereich des Diagramms befindet sich eine Zeitleiste, welche die Systemaktivität in Echtzeit innerhalb des gewählten Zeitraums aufzeichnet. Um den Zeitraum zu ändern, klicken Sie auf die Option **Schritt: 1...** unten rechts im Fenster.



Folgende Optionen stehen zur Verfügung:

- **Schritt: 1 Sekunde (letzte 10 Minuten)** - Das Diagramm wird jede Sekunde aktualisiert. Die Zeitleiste deckt die letzten 10 Minuten.
- **Schritt: 1 Minute (letzte 24 Stunden)** - Das Diagramm wird jede Minute aktualisiert. Die Zeitleiste deckt die letzten 24 Stunden.
- **Schritt: 1 Stunde (letzter Monat)** - Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste deckt den letzten Monat.
- **Schritt: Schritt: 1 Stunde (ausgewählter Monat)** - Das Diagramm wird jede Stunde aktualisiert. Die Zeitleiste deckt die X letzten, ausgewählten Monate.

Die vertikale Achse im **Systemaktivitätsdiagramm** bildet die gelesenen (blau) und geschriebenen Daten (rot) ab. Beide Werte werde in KB (Kilobyte)/MB/GB angegeben. Wenn Sie mit dem Mauszeiger über die gelesenen oder geschriebenen Daten in der Legende unterhalb des Diagramms fahren, werden im Diagramm nur die Daten für diesen Aktivitätstyp angezeigt.

Alternativ können Sie **Netzwerkaktivität** im Dropdown-Menü **Aktivität** auswählen. Die Anzeige und die Einstellungen der Diagramme für **Systemaktivität** und **Netzwerkaktivität** sind fast identisch. Bei der Netzwerkaktivität werden empfangene (rot) und gesendete Daten (blau) dargestellt.

4.6.5 ESET SysInspector

ESET SysInspector ist eine Anwendung, die Ihren Computer gründlich durchsucht und eine genaue (Risikostufen-) Analyse Ihrer Systemkomponenten erstellt. Hierzu zählen u. a. installierte Treiber und Anwendungen, Netzwerkverbindungen oder wichtige Registrierungseinträge. Diese Informationen helfen Ihnen beim Aufspüren der Ursache für verdächtiges Systemverhalten, welches möglicherweise durch Software- oder Hardwareinkompatibilität oder eine Infektion mit Schadcode hervorgerufen wurde.

Das Fenster „SysInspector“ zeigt folgende Informationen zu erstellten Logs an:

- **Zeit** - Zeitpunkt der Log-Erstellung
- **Kommentar** - Eine kurze Beschreibung
- **Benutzer** - Der Name des Benutzers, der das Log erstellt hat
- **Status** - Status bei der Log-Erstellung

Folgende Aktionen stehen zur Verfügung:

- **Vergleichen** - Vergleich zweier vorhandener Logs
- **Erstellen** - Erstellen eines neuen Logs Warten Sie, bis das ESET SysInspector-Log erstellt wurde (**Status** ist „Erstellt“).
- **Löschen** - Löschen von ausgewählten Logs aus der Liste.

Mit einem Rechtsklick auf ein oder mehrere ausgewählte Logs stehen im Kontextmenü die folgenden Optionen zur Verfügung:

- **Anzeigen** - Anzeige des ausgewählten Logs in ESET SysInspector (entspricht einem Doppelklick auf einen beliebigen Eintrag)
- **Alle löschen** - Löschen aller Logs
- **Exportieren** - Exportieren des Logs in eine *.xml*-Datei oder eine komprimierte *.xml*-Datei

4.6.6 ESET Live Grid

ESET Live Grid basiert auf dem ESET ThreatSense.Net Frühwarnsystem und arbeitet mit von ESET-Anwendern weltweit übermittelten Daten, die es an das ESET-Virenlabor sendet. ESET Live Grid stellt verdächtige Proben und Metadaten „aus freier Wildbahn“ bereit und gibt uns so die Möglichkeit, unmittelbar auf die Anforderungen unserer Kunden zu reagieren und sie vor den neuesten Bedrohungen zu schützen. Weitere Informationen zu ESET Live Grid finden Sie in unserem Glossar.

Benutzer können sich direkt im Programmfenster oder im jeweiligen Kontextmenü anzeigen lassen, wie ausgeführte Prozesse oder Dateien eingeschätzt werden. Zudem sind über ESET Live Grid weitere Informationen verfügbar. Als Benutzer haben Sie zwei Möglichkeiten:

1. Sie haben die Möglichkeit, ESET Live Grid nicht zu aktivieren. Ihnen steht der volle Funktionsumfang der Software zur Verfügung, und Sie erhalten auch in diesem Fall den besten Schutz, den wir Ihnen bieten können.
2. Sie können ESET Live Grid so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Die Informationen bleiben anonym. Diese Datei kann zur detaillierten Analyse an ESET gesendet werden. Durch die Untersuchung dieser Bedrohungen kann ESET die Fähigkeit seiner Software zur Erkennung von Schadsoftware aktualisieren und verbessern.

ESET Live Grid sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Dazu können auch Proben oder Kopien der Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers.

ESET Smart Security ist standardmäßig so konfiguriert, dass verdächtige Dateien zur genauen Analyse an ESET eingereicht werden. Dateien mit bestimmten Erweiterungen (z. B. *.doc* oder *.xls*) sind immer von der Übermittlung ausgeschlossen. Sie können andere Dateierweiterungen hinzufügen, wenn es bestimmte Dateitypen gibt, die Sie oder Ihr Unternehmen nicht übermitteln möchten.

Das Einstellungsmenü für ESET Live Grid bietet verschiedene Optionen zum Aktivieren/Deaktivieren von ESET Live Grid, mit dem verdächtige Dateien und anonyme statistische Daten an ESET übermittelt werden. Um darauf zuzugreifen, klicken Sie in der Baumstruktur der erweiterten Einstellungen auf **Tools** > **ESET Live Grid**.

An ESET Live Grid teilnehmen (empfohlen) - Aktiviert/deaktiviert ESET Live Grid, mit dem verdächtige Dateien und anonyme statistische Daten an ESET übermittelt werden.

Keine statistischen Daten einreichen - Wählen Sie diese Option, wenn Sie mit ESET Live Grid keine statistischen Daten über Ihren Computer senden möchten. Dabei handelt es sich um Informationen zu neu erkannten Bedrohungen. Erfasst werden: Name der Bedrohung, Datum und Uhrzeit der Erkennung, Versionsnummer von ESET Smart Security, Versionsdaten und Regionseinstellung des Betriebssystems. Statistiken werden normalerweise einmal oder zweimal täglich an ESET übermittelt.

Keine Dateien einreichen - Verdächtige Dateien, deren Inhalt oder Verhalten auf eingedrungenen Schadcode hinweist, werden nicht über die ESET Live Grid-Technologie zur Analyse an ESET übermittelt.

Erweiterte Einstellungen... - Ein Dialogfenster mit zusätzlichen Einstellungen für ESET Live Grid wird angezeigt.

Wenn Sie ESET Live Grid einige Zeit verwendet haben, kann es sein, dass auch nach dem Deaktivieren des Systems noch einige Datenpakete zum Senden vorliegen. Zum nächstmöglichen Zeitpunkt werden diese Pakete an ESET übermittelt. Es werden aber keine neuen Pakete mehr erstellt.

4.6.6.1 Verdächtige Dateien

In der Registerkarte **Dateien** in den erweiterten Einstellungen von ESET Live Grid können Sie konfigurieren, wie Bedrohungen zur Analyse an ESET gesendet werden.

Wenn Sie eine verdächtige Datei finden, können Sie sie zur Analyse an unser Virenlabor einreichen. Sollte dabei schädlicher Code zu Tage treten, wird dieser beim nächsten Update der Signaturdatenbank berücksichtigt.

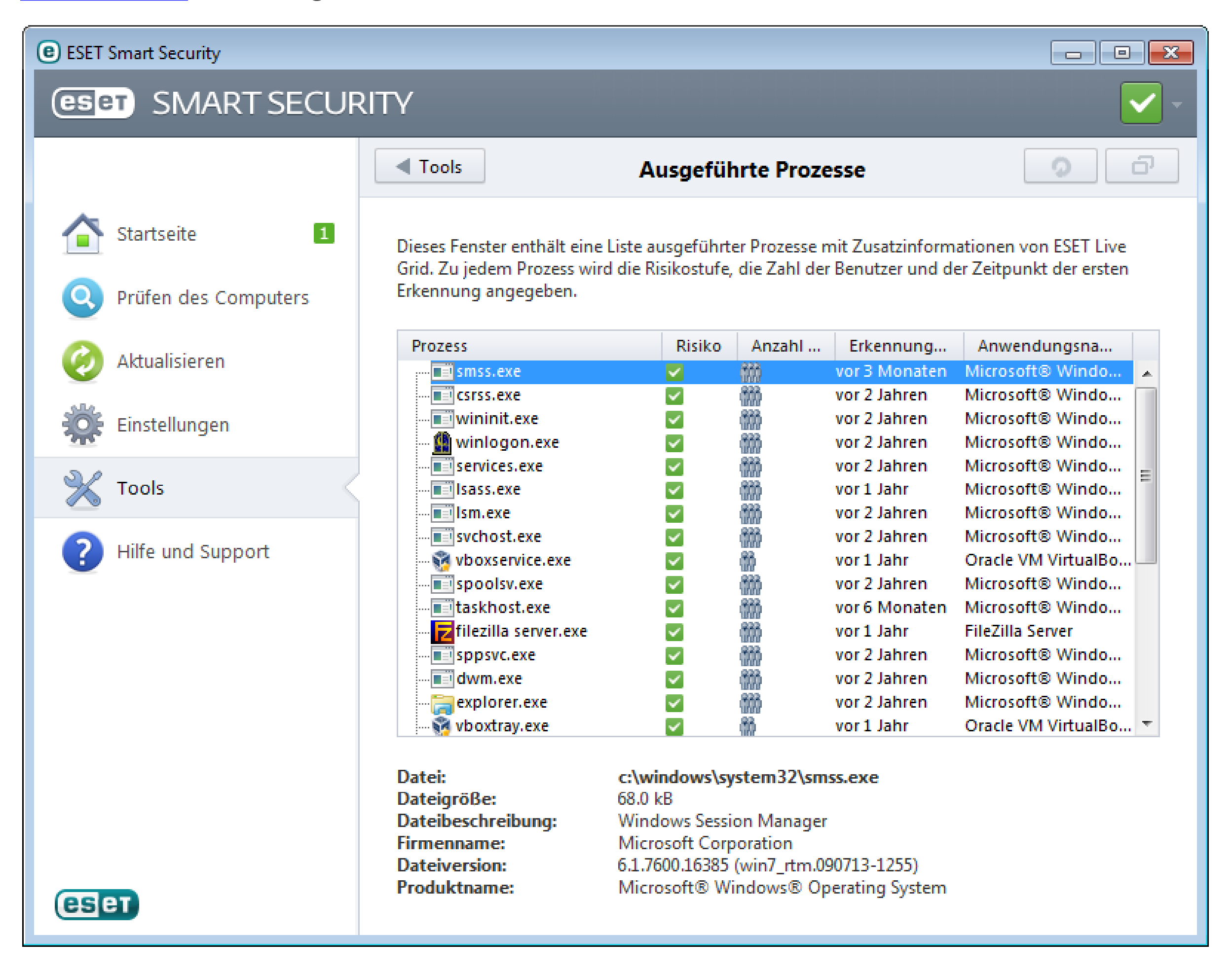
Ausschlussfilter - Über diese Option können Sie bestimmte Dateien oder Ordner vom Senden ausschließen. Hier eingetragene Dateien werden nicht an ESET übermittelt, auch wenn sie verdächtigen Code enthalten. Hier können Dateien eingetragen werden, die eventuell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc usw.). Sie können der Ausschlussliste weitere Dateien hinzufügen.

E-Mail-Adresse für Rückfragen (optional) - Sie können mit den verdächtigen Dateien eine E-Mail-Adresse für Rückfragen angeben, wenn zur Analyse weitere Informationen erforderlich sind. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

Wählen Sie die Option **Erstellen von Logs aktivieren** aus, um einen Event Log zu erstellen, in dem alle Informationen über das Einreichen von Dateien und statistischen Daten protokolliert werden. Dadurch werden Einträge im Ereignis-Log erstellt, wenn Dateien oder statistische Daten eingereicht werden.

4.6.7 Ausgeführte Prozesse

Die Informationen zu ausgeführten Prozessen zeigen die auf dem Computer ausgeführten Programme und Prozesse an und stellen dem ESET-Produkt laufend aktuelle Informationen zu neuen Infiltrationen bereit. ESET Smart Security bietet ausführliche Informationen zu ausgeführten Prozessen, um den Benutzern den Schutz der ESET Live Grid-Technologie zu bieten.



Prozess - Zeigt den Namen des Programms oder Prozesses an, das/der derzeit auf dem Computer ausgeführt wird. Sie können alle auf Ihrem Computer ausgeführten Prozesse auch über den Windows-Taskmanager anzeigen. Öffnen Sie den Taskmanager, indem Sie mit der rechten Maustaste auf einen leeren Bereich auf der Taskleiste und

dann auf **Taskmanager** klicken oder indem Sie Strg+Umschalt+Esc auf Ihrer Tastatur drücken.

Risikostufe - Um Objekten wie Dateien, Prozessen, Registrierungsschlüsseln usw. eine Risikostufe zuzuordnen, verwenden ESET Smart Security und die ESET Live Grid-Technologie in der Regel einen Satz heuristischer Regeln, mit denen die Merkmale des Objekts untersucht werden, um anschließend nach entsprechender Gewichtung das Potenzial für schädliche Aktivitäten abzuschätzen. Basierend auf dieser Heuristik wird Objekten dann eine Risikostufe zugewiesen, von 1 - In Ordnung (grün) bis 9 - Risikoreich(rot).

HINWEIS: Bekannte Anwendungen, die als In Ordnung (grün) markiert sind, sind in jedem Fall sauber (Positivliste) und werden von der Prüfung ausgenommen. Dadurch wird die Geschwindigkeit der On-Demand-Prüfung bzw. des Echtzeit-Dateischutzes auf Ihrem Computer erhöht.

Anzahl Benutzer - Die Anzahl der Benutzer, die eine bestimmte Anwendung verwenden. Diese Informationen werden von der ESET Live Grid-Technologie gesammelt.

Erkennungszeitpunkt - Zeitspanne seit der Erkennung der Anwendung durch die ESET Live Grid-Technologie.

HINWEIS: Wenn eine Anwendung als Unbekannt (orange) eingestuft wurde, muss es sich nicht zwangsläufig um Schadsoftware handeln. In der Regel ist es einfach eine neuere Anwendung. Wenn Sie sich bei einer Datei unsicher sind, können Sie diese über die Funktion Dateien zur Analyse einreichen an ESET einreichen. Wenn sich herausstellt, dass die Datei Schadcode enthält, werden entsprechende Erkennungsfunktionen in zukünftigen Updates berücksichtigt.

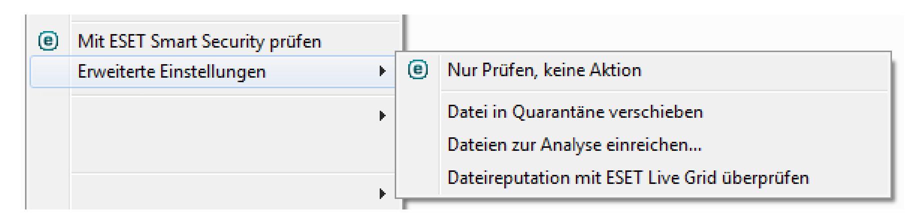
Anwendungsname - Der Name eines Programms oder Prozesses.

In neuem Fenster anzeigen - Die Informationen zu den ausgeführten Prozessen werden in einem neuen Fenster angezeigt.

Wenn Sie unten auf eine Anwendung klicken, werden unten im Fenster die folgenden Informationen angezeigt:

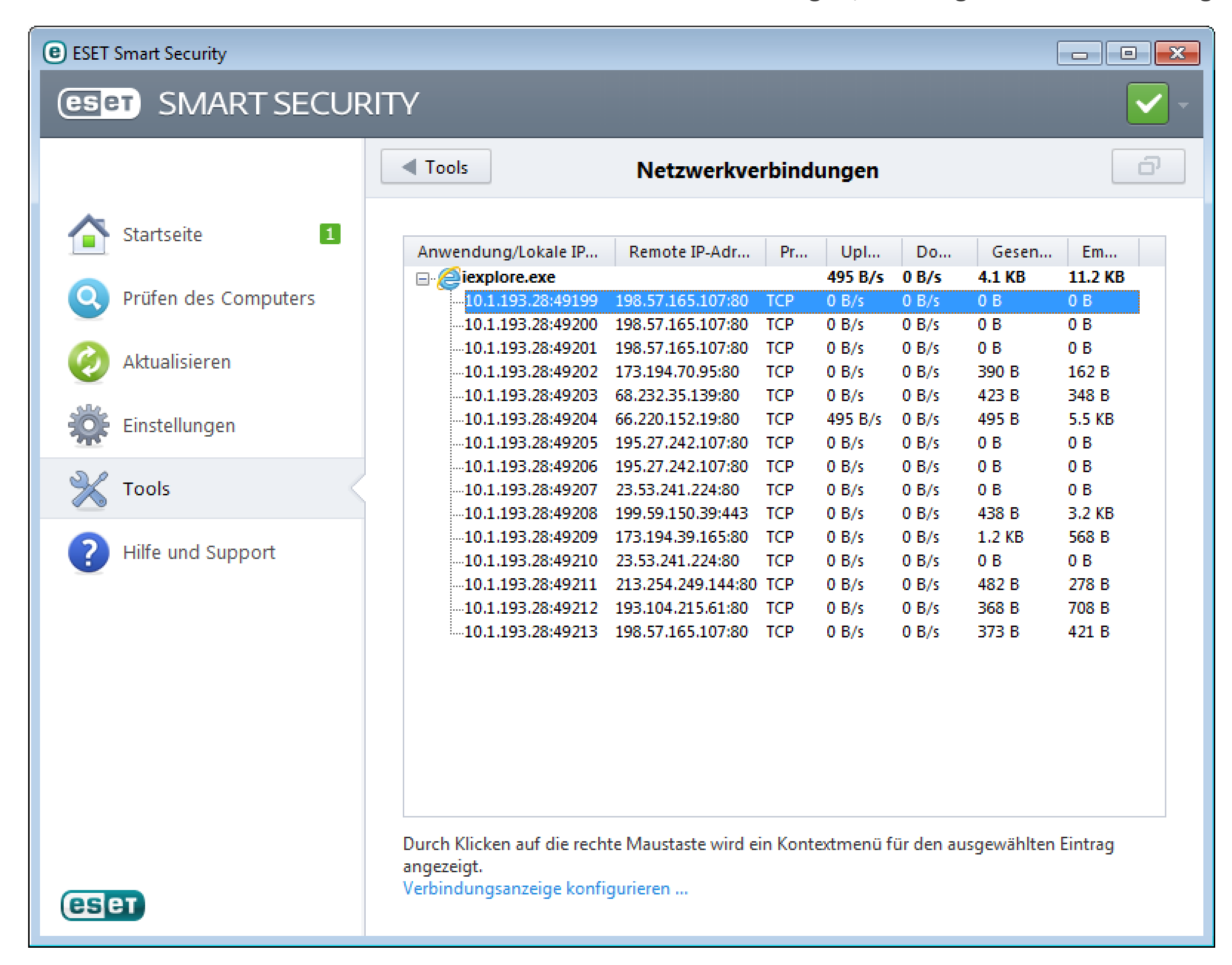
- **Datei** - Speicherort einer Anwendung auf Ihrem Computer
- **Dateigröße** - Dateigröße in B (Byte).
- **Dateibeschreibung** - Dateieigenschaften auf Grundlage der Beschreibung des Betriebssystems
- **Firmenname** - Name des Herstellers oder des Anwendungsprozesses
- **Dateiversion** - Information vom Herausgeber der Anwendung
- **Produktname** - Name der Anwendung und/oder Firmenname

HINWEIS: Der Reputations-Check kann auch auf Dateien angewendet werden, die nicht als Programme/Prozesse ausgeführt werden. - Markieren Sie die Dateien, die Sie überprüfen möchten, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Erweiterte Einstellungen** > **Dateireputation mit ESET Live Grid überprüfen** aus.



4.6.8 Netzwerkverbindungen

Im Abschnitt „Netzwerkverbindungen“ wird eine Liste der aktiven und der ausstehenden Verbindungen angezeigt. Auf diese Weise behalten Sie die Übersicht über alle Anwendungen, die ausgehende Verbindungen herstellen.



In der ersten Zeile werden der Name der Anwendung und die Geschwindigkeit der Datenübertragung angezeigt. Zum Anzeigen einer Liste der von der Anwendung hergestellten Verbindungen (und weiterer Informationen) klicken Sie auf **+**.

Anwendung/Lokale IP-Adresse - Name der Anwendung, lokale IP-Adressen und für die Datenübertragung verwendete Ports

Remote IP-Adresse - IP-Adresse und Portnummer eines bestimmten Remotecomputers

Protokoll - Verwendetes Übertragungsprotokoll

Uploadgeschwindigkeit/Downloadgeschwindigkeit - Aktuelle Übertragungsgeschwindigkeit eingehender bzw. ausgehender Daten

Gesendet/Empfangen - Über die Verbindung übertragene Datenmenge

In neuem Fenster öffnen - Anzeigen der Informationen in einem neuen Fenster

Die Option **Einstellungen für Verbindungsanzeige...** im Bildschirm Netzwerkverbindungen öffnet die erweiterten Einstellungen für diesen Abschnitt. Hier können Sie Verbindungsanzeigeoptionen ändern:

Hostnamen anzeigen - Falls möglich, werden anstelle der IP-Adressen die DNS-Namen von Gegenstellen angezeigt.

Nur TCP-Verbindungen anzeigen - Die Liste enthält nur Verbindungen, die ein TCP-Protokoll verwenden.

Eingehende offene Ports anzeigen - Wählen Sie diese Option aus, um nur Verbindungen anzuzeigen, für die aktuell keine Kommunikation erfolgt, das System jedoch einen Port geöffnet hat und auf eine Verbindung wartet.

Verbindungen innerhalb des Computers anzeigen - Aktivieren Sie diese Option, um nur Verbindungen anzuzeigen, bei denen die Gegenstelle der eigene Computer ist (so genannte *Localhost*-Verbindungen).

Klicken Sie mit der rechten Maustaste auf eine Verbindung. Es werden Ihnen zusätzliche Optionen angezeigt:

Kommunikation für Verbindung blockieren - Beendet die aufgebaute Verbindung Diese Option steht erst zur Verfügung, nachdem Sie eine aktive Verbindung angeklickt haben.

Details anzeigen - Durch Aktivieren dieser Option werden weitere Informationen zur ausgewählten Verbindung angezeigt.

Aktualisierungsintervall - Wählen Sie das Intervall für die Aktualisierung der aktiven Verbindungen.

Jetzt aktualisieren - Lädt das Fenster „Netzwerkverbindungen“ neu.

Die folgenden Optionen stehen erst zur Verfügung, nachdem Sie eine Anwendung oder einen Prozess angeklickt haben, d. h. nicht eine aktive Verbindung:

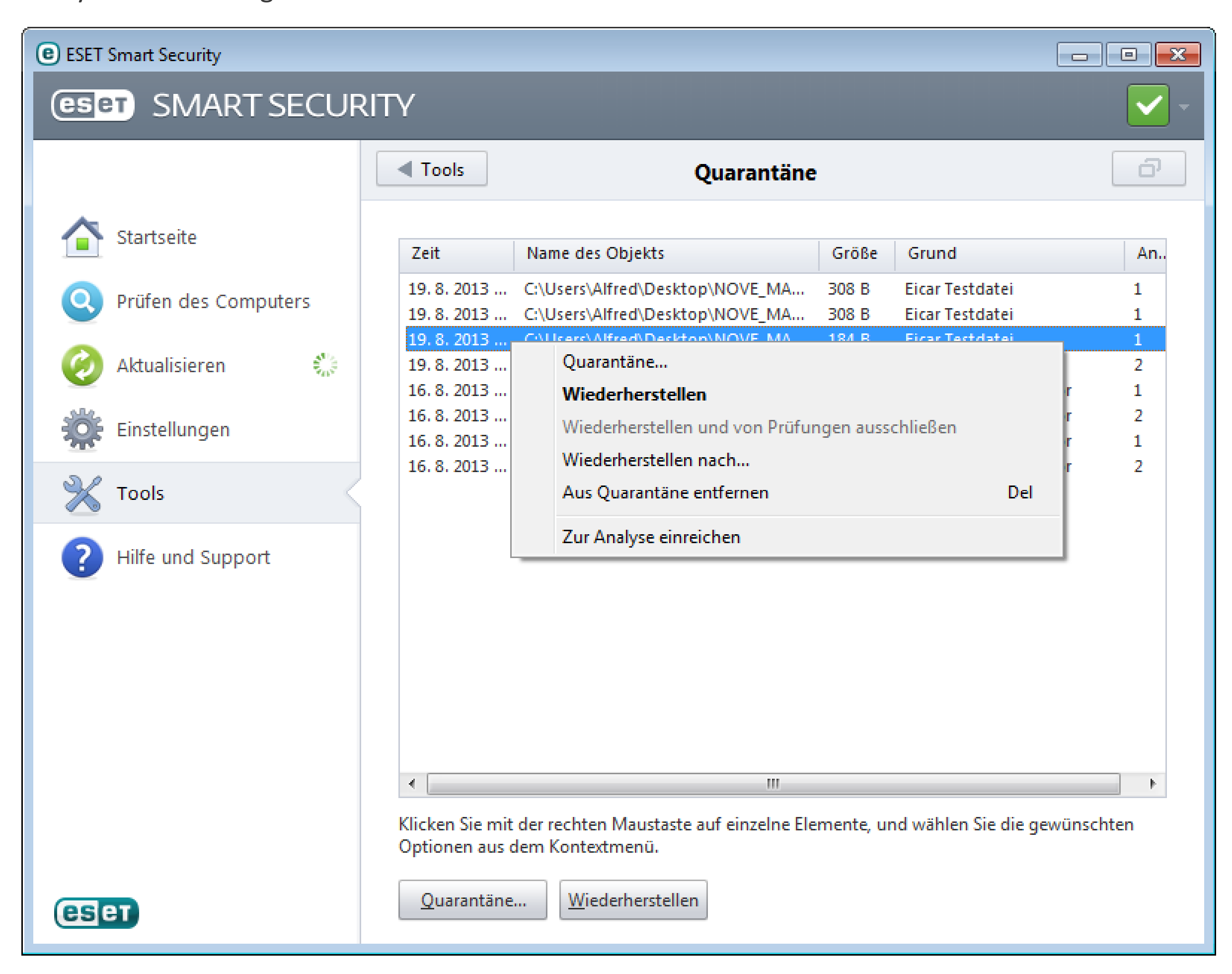
Kommunikation für Prozess vorübergehend blockieren - Verbindungen für diese Anwendung werden vorübergehend blockiert. Wenn eine neue Verbindung hergestellt wird, verwendet die Firewall eine vordefinierte Regel. Eine Beschreibung der Einstellungen finden Sie im Abschnitt Regeln und Zonen.

Kommunikation für Prozess vorübergehend zulassen - Verbindungen für diese Anwendung werden vorübergehend zugelassen. Wenn eine neue Verbindung hergestellt wird, verwendet die Firewall eine vordefinierte Regel. Eine Beschreibung der Einstellungen finden Sie im Abschnitt Regeln und Zonen.

4.6.9 Quarantäne

Die Hauptfunktion der Quarantäne ist die sichere Verwahrung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Smart Security fälschlicherweise erkannt worden sind.

Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch nicht erkannt werden. Dateien aus der Quarantäne können zur Analyse an ESET eingereicht werden.



Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der

Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (z. B. Objekt hinzugefügt durch Benutzer) und die Anzahl der Bedrohungen (z. B. bei Archiven, in denen an mehreren Stellen Schadcode erkannt wurde) enthält.

Quarantäne für Dateien

ESET Smart Security kopiert gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Quarantäne** klicken. In diesem Fall wird die Originaldatei nicht von ihrem ursprünglichen Speicherort entfernt. Alternativ kann auch das Kontextmenü zu diesem Zweck verwendet werden: Klicken Sie mit der rechten Maustaste in das Fenster **Quarantäne**, und wählen Sie **Quarantäne**.

Wiederherstellen aus Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Dazu verwenden Sie die Funktion **Wiederherstellen** im Kontextmenü, das angezeigt wird, wenn Sie im Fenster „Quarantäne" mit der rechten Maustaste auf eine entsprechende Datei klicken. Wenn eine Datei als eventuell unerwünschte Anwendung markiert ist, wird die Option **Wiederherstellen und von Prüfungen ausschließen** aktiviert. Weitere Informationen zu diesem Anwendungstyp finden Sie im Glossar. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

HINWEIS: Wenn versehentlich eine harmlose Datei in Quarantäne versetzt wurde, schließen Sie die Datei nach der Wiederherstellung von der Prüfung aus und senden Sie sie an den ESET-Support.

Einreichen einer Datei aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in Quarantäne versetzt haben oder wenn eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an ESET. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, klicken Sie mit der rechten Maustaste darauf und wählen im angezeigten Kontextmenü die Option **Datei zur Analyse einreichen**.

4.6.10 Einstellungen für Proxyserver

In großen lokalen Netzwerken wird die Verbindung zum Internet häufig über Proxyserver vermittelt. Wenn dies der Fall ist, müssen die nachfolgend beschriebenen Einstellungen vorgenommen werden. Wenn die Einstellungen nicht vorgenommen werden, ist es möglicherweise nicht möglich, automatisch Updates über das Internet zu beziehen. ESET Smart Security bietet Optionen für die Proxyserver-Einstellungen in zwei verschiedenen Bereichen der erweiterten Einstellungen.

Die Einstellungen für den Proxyserver können zum einen in **Erweiterte Einstellungen** unter **Tools** > **Proxyserver** konfiguriert werden. So legen Sie die allgemeinen Proxyserver-Einstellungen für alle Funktionen von ESET Smart Security fest. Diese Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet benötigen.

Um die Proxyserver-Einstellungen für diese Ebene festzulegen, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende Adresse zusammen mit dem **Port** des Proxyservers ein.

Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie das Kontrollkästchen **Proxyserver erfordert Authentifizierung** und geben einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein. Klicken Sie auf die Schaltfläche **Proxyserver automatisch erkennen**, wenn die Einstellungen des Proxyservers automatisch erkannt und ausgefüllt werden sollen. Die in Internet Explorer festgelegten Einstellungen werden kopiert.

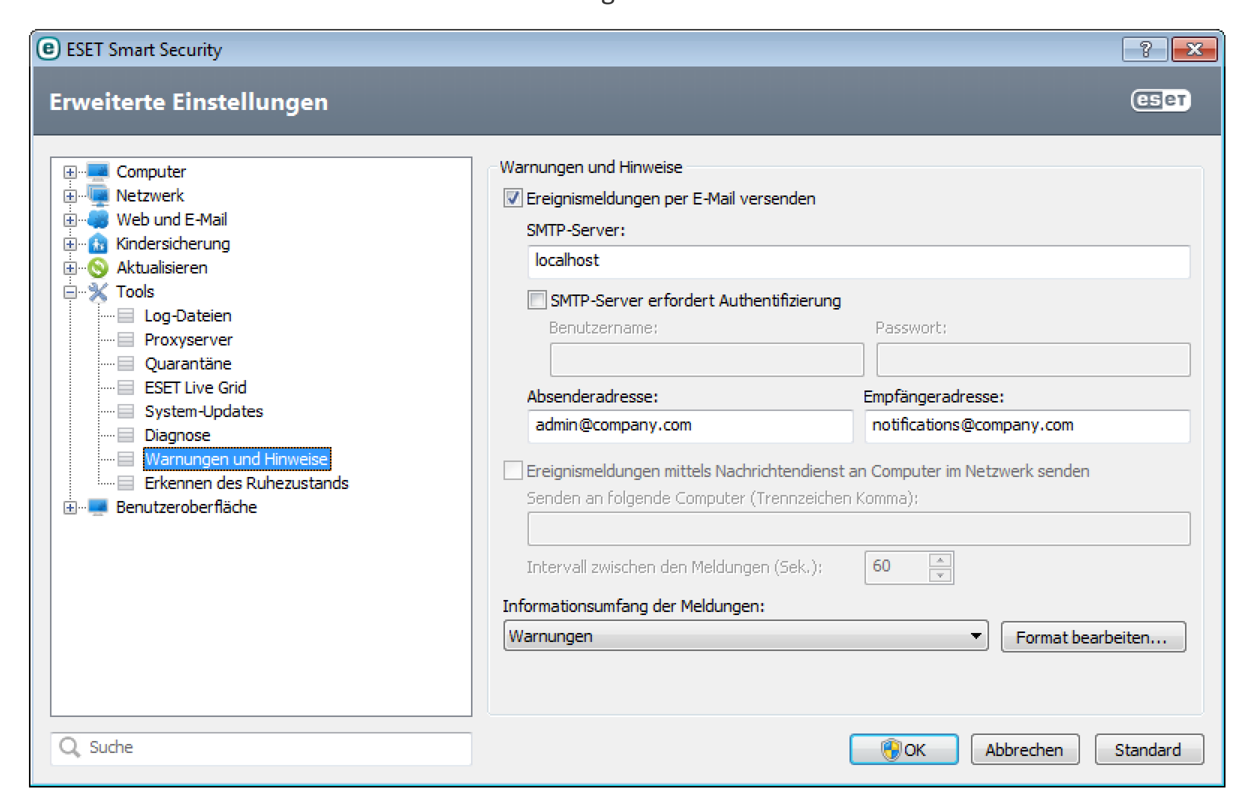
HINWEIS: Diese Funktion ruft keine Anmeldedaten (Benutzername und Passwort) ab; Sie müssen diese Informationen eingeben.

Die Proxyserver-Einstellungen können auch in den erweiterten Einstellungen für Updates festgelegt werden (**Update** unter **Erweiterte Einstellungen**). Die Einstellungen gelten dann für das entsprechende Update-Profil; diese Methode wird für Laptops empfohlen, da diese die Updates der Signaturdatenbank oft von verschiedenen Quellen beziehen. Weitere Informationen zu diesen Einstellungen finden Sie im Abschnitt Erweiterte Einstellungen für

[Updates](#).

4.6.11 Warnungen und Hinweise

ESET Smart Security unterstützt das Senden von E-Mails, wenn ein Ereignis mit dem ausgewählten Informationsumfang auftritt. Aktivieren Sie das Kontrollkästchen **Ereignismeldungen per E-Mail versenden**, um diese Funktion und die E-Mail-Hinweismeldungen zu aktivieren.



SMTP-Server - Der SMTP-Server, über den Meldungen per E-Mail verschickt werden sollen.

Hinweis: ESET Smart Security unterstützt keine SMTP-Server mit SSL/TLS-Verschlüsselung.

SMTP-Server erfordert Authentifizierung - Falls für den SMTP-Server Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie hier einen gültigen Benutzernamen und das Passwort ein.

Absenderadresse - Dieses Feld enthält die Adresse, die in Ereignismeldungen als Absender verzeichnet sein soll.

Empfängeradresse - Dieses Feld enthält die Adresse, die in Ereignismeldungen als Empfänger verzeichnet sein soll.

Ereignismeldungen mittels Nachrichtendienst an Computer im Netzwerk senden - Aktivieren Sie dieses Kontrollkästchen, um Meldungen mit dem Windows®-Messaging-Dienst an andere Computer im Netzwerk zu übertragen.

Senden an folgende Computer (Trennzeichen Komma) - Geben Sie die Namen der Computer ein, an die Ereignismeldungen über den Windows®-Nachrichtendienst verschickt werden sollen.

Intervall zwischen den Meldungen (Sek.) - Legen Sie den Zeitabstand zwischen Sendevorgängen fest.

Informationsumfang der Meldungen - Hier können Sie festlegen, welche Ereignistypen das Versenden von Meldungen auslösen sollen.

Format bearbeiten - Ereignismeldungen werden an Remotebenutzer/Administratoren als E-Mails oder LAN-Nachrichten (Windows®-Messaging-Dienst) weitergeleitet. Das Standard-Nachrichtenformat ist für die meisten Einsatzfälle ausreichend. Sie können es jedoch auch anpassen. - Klicken Sie hierzu auf [Format bearbeiten](#).

4.6.11.1 Format von Meldungen

Hier können Sie das Format der Ereignismeldungen festlegen, die auf Remote-Computern angezeigt werden.

Warnungen und Hinweismeldungen besitzen ein vordefiniertes Standardformat. Dieses Format sollte nicht geändert werden. Unter bestimmten Umständen (etwa, wenn Sie ein automatisiertes E-Mail-Verarbeitungssystem verwenden) ist es jedoch möglicherweise erforderlich, das Meldungsformat zu ändern.

Schlüsselwörter (durch %-Zeichen abgetrennte Zeichenfolgen) in der Meldung werden durch entsprechende Informationen ersetzt. Folgende Schlüsselwörter sind verfügbar:

- **%TimeStamp%** - Datum und Uhrzeit des Ereignisses
- **%Scanner%** - Betroffenes Modul
- **%ComputerName%** - Name des Computers, auf dem die Warnmeldung aufgetreten ist
- **%ProgramName%** - Programm, das die Warnung erzeugt hat
- **%InfectedObject%** - Name der infizierten Datei, Nachricht usw.
- **%VirusName%** - Angabe des Infektionsverursachers
- **%ErrorDescription%** - Beschreibung eines nicht durch Viruscode ausgelösten Ereignisses

Die Schlüsselwörter **%InfectedObject%** und **%VirusName%** werden nur in Warnmeldungen bei Bedrohungen verwendet, **%ErrorDescription%** nur in Ereignismeldungen.

Lokalen Zeichensatz verwenden - Konvertiert eine E-Mail-Nachricht anhand der Ländereinstellungen in Windows in eine ANSI-Zeichenkodierung (z. B. Windows-1250). Wenn Sie diese Option deaktiviert lassen, werden Nachrichten in 7-Bit-ACSII kodiert (dabei wird z. B. „à“ zu „a“ geändert und ein unbekanntes Symbol durch ein Fragezeichen ersetzt).

Lokale Zeichenkodierung verwenden - Die E-Mail-Nachrichtenquelle wird in das QP-Format konvertiert, das ASCII-Zeichen verwendet und besondere regionale Zeichen in der E-Mail korrekt im 8-Bit-Format überträgt (áéíóú).

4.6.12 Proben zur Analyse einreichen

Über das Dialogfenster zum Dateiversand können Sie Dateien bei ESET zur Analyse einreichen. Sie öffnen es unter **Tools** > **Probe zur Analyse einreichen**. Wenn Ihnen eine Datei auf Ihrem Computer oder eine Webseite verdächtig erscheint, können Sie die Datei zur Analyse an ESET senden. Wenn sich herausstellt, dass die Datei bzw. Webseite Schadcode enthält, werden entsprechende Erkennungsfunktionen in zukünftigen Updates berücksichtigt.

Sie können Dateien auch per E-Mail einsenden. Komprimieren Sie in diesem Fall die Datei(en) mit WinRAR/WinZIP, verschlüsseln Sie das Archiv mit dem Passwort „infected“ und senden Sie es an samples@eset.com. Formulieren Sie eine aussagekräftige Betreffzeile, und notieren Sie möglichst viele ergänzende Informationen zu den eingesandten Dateien (z. B. von welcher Website Sie die Dateien heruntergeladen haben).

HINWEIS: Auf Dateien, die Sie an ESET senden, sollte mindestens eines der folgenden Kriterien zutreffen:
- Die Datei wird nicht als Bedrohung erkannt
- Die Datei wird als Bedrohung erkannt, obwohl Sie keinen Schadcode enthält

ESET wird nur dann Kontakt mit Ihnen aufnehmen, wenn zusätzliche Angaben für die Dateianalyse benötigt werden.

Wählen Sie aus dem Dropdownmenü **Grund für Einreichen der Datei** die Beschreibung aus, die am besten auf Ihre Mitteilung zutrifft:
- **Verdächtige Datei**
- **Verdächtige Website** (eine Website, die mit Schadsoftware infiziert ist)
- **Fehlalarm Datei** (als Bedrohung erkannte Datei, die jedoch nicht infiziert ist)
- **Fehlalarm Webseite**
- **Sonstige**

Datei/Webseite - Der Pfad zu der Datei oder Webseite, die eingesandt werden soll.

E-Mail-Adresse - Diese E-Mail-Adresse wird zusammen mit verdächtigen Dateien an ESET übermittelt. Möglicherweise wird ESET über diese Adresse Kontakt mit Ihnen aufnehmen, wenn zusätzliche Angaben für die Dateianalyse benötigt werden. Diese Angabe ist freiwillig. Sie werden nur im Ausnahmefall eine Antwort von ESET

erhalten, da täglich mehrere Zehntausend Dateien auf unseren Servern eingehen und wir nicht jede Meldung individuell beantworten können.

4.6.13 System-Updates

Die Windows Update-Funktion ist ein wichtiger Bestandteil des Schutzes vor bösartiger Software. Aus diesem Grund ist es essenziell, dass Sie verfügbare Microsoft Windows-Updates sofort installieren. Entsprechend der von Ihnen festgelegten Richtlinien benachrichtigt Sie ESET Smart Security über fehlende Updates. Folgende Richtlinien sind verfügbar:

- **Keine Updates** - Es werden keine Updates zum Download angeboten.
- **Optionale Updates** - Updates mit beliebiger Priorität werden zum Download angeboten.
- **Empfohlene Updates** - Updates mit normaler Priorität und höher werden zum Download angeboten.
- **Wichtige Updates** - Updates mit hoher Priorität und kritische Updates werden zum Download angeboten.
- **Kritische Updates** - Nur kritische Updates werden zum Download angeboten.

Klicken Sie auf **OK**, um die Änderungen zu speichern. Das Fenster „System-Updates“ wird nach erfolgter Statusverifizierung durch den Update-Server angezeigt. Dementsprechend stehen die aktualisierten Systemdaten möglicherweise nicht unmittelbar nach Speicherung der Änderungen zur Verfügung.

4.7 Benutzeroberfläche

Im Abschnitt **Benutzeroberfläche** können Sie das Verhalten der grafischen Benutzeroberfläche (GUI) des Programms konfigurieren.

Mit Grafik können Sie die Darstellung und die Effekte des Programms ändern.

Konfigurieren Sie Warnungen und Hinweise, um festzulegen, wie Warnungen bei erkannten Bedrohungen und Systemhinweise angezeigt werden sollen. So können Sie diese Funktion Ihren Anforderungen anpassen.

Wenn Sie festlegen, dass bestimmte Hinweise nicht angezeigt werden sollen, werden diese in die Liste Versteckte Hinweisfenster aufgenommen. Hier können Sie den Status der Hinweise einsehen, sie detaillierter anzeigen lassen oder sie aus dem Fenster entfernen.

Um Ihre Sicherheitssoftware bestmöglich zu schützen und unerlaubte Änderungen zu vermeiden, können Sie mit der Funktion Einstellungen für den Zugriff einen Passwortschutz für Ihre Einstellungen einrichten.

Das Kontextmenü wird angezeigt, wenn Sie mit der rechten Maustaste auf ein Element klicken. Mit diesem Tool können ESET Smart Security-Steuerelemente in das Kontextmenü integriert werden.

4.7.1 Grafik

Über die Konfigurationsoptionen für die Benutzeroberfläche von ESET Smart Security können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Um auf diese Konfigurationsoptionen zuzugreifen, erweitern Sie in den erweiterten Einstellungen den Eintrag **Benutzeroberfläche** und klicken Sie auf **Grafik**.

Im Bereich **Elemente der Benutzeroberfläche** sollte die Option **Grafische Benutzeroberfläche** deaktiviert werden, wenn durch die grafischen Elemente die Leistung des Computers beeinträchtigt wird oder andere Probleme auftreten. Die grafische Oberfläche sollte ebenso für sehbehinderte Personen deaktiviert werden, da Konflikte mit Spezialanwendungen zum Vorlesen von Text auf dem Bildschirm auftreten können.

Wenn ESET Smart Security ohne Anzeige des Startbilds gestartet werden soll, deaktivieren Sie die Option **Startbild anzeigen**.

Durch Aktivieren der Option **Aktives Steuerelement auswählen** wird jedes Element hervorgehoben, das sich gerade im aktiven Bereich des Mauszeigers befindet. Mit einem Klick wird das hervorgehobene Element aktiviert.

Um bei der Ausführung verschiedener Vorgänge animierte Symbole anzuzeigen, aktivieren Sie die Option **Animierte Symbole für Fortschrittsanzeige verwenden**.

Wenn ESET Smart Security bei wichtigen Ereignissen wie z. B. der Erkennung einer Bedrohung oder wenn eine Prüfung abgeschlossen wird, einen Warnton ausgeben soll, aktivieren Sie die Option **Hinweistöne wiedergeben**.

4.7.2 Warnungen und Hinweise

Im Bereich **Warnungen und Hinweise** unter **Benutzeroberfläche** können Sie festlegen, wie ESET Smart Security mit Bedrohungswarnungen und Systemmeldungen (z. B. über erfolgreiche Updates) umgehen soll. Außerdem können Sie Anzeigedauer und Transparenz von Meldungen in der Taskleiste festlegen (nur bei Systemen, die Meldungen in der Taskleiste unterstützen).

Deaktivieren Sie das Kontrollkästchen neben **Fenster mit Warnungen anzeigen**, um das Anzeigen aller Warnungsfenster zu unterbinden. Diese Option ist nur für besondere Situationen geeignet. Für die meisten Benutzer empfiehlt es sich, die Option aktiviert zu lassen (Standardeinstellung).

Hinweise auf dem Desktop dienen ausschließlich zu Informationszwecken; Eingaben des Benutzers sind weder möglich noch erforderlich. Sie werden im Infobereich der Taskleiste rechts unten auf dem Bildschirm angezeigt. Zum Aktivieren von Desktophinweisen aktivieren Sie die Option **Hinweise auf dem Desktop anzeigen**. Weitere Optionen, wie Anzeigedauer und Transparenz, lassen sich einstellen, indem Sie auf **Hinweise konfigurieren** klicken. Um eine Vorschau des Verhaltens von Hinweisen zu erhalten, klicken Sie auf **Vorschau**. Wählen Sie **Desktophinweise nicht anzeigen, wenn Anwendungen im Vollbildmodus ausgeführt werden**, um die Hinweise beim Ausführen von Anwendungen im Vollbildmodus zu unterdrücken.

Wenn Popup-Fenster nach einer bestimmten Zeit automatisch geschlossen werden sollen, aktivieren Sie die Option **Fenster mit Hinweisen schließen nach (Sek.)**. Die Hinweise werden nach Ablauf der festgelegten Zeit automatisch geschlossen, sofern sie nicht bereits vom Benutzer geschlossen wurden.

Klicken Sie auf **Erweiterte Einstellungen**, um auf zusätzliche Einstellungen für **Warnungen und Hinweise** zuzugreifen.

4.7.2.1 Erweiterte Einstellungen

Aus der Liste **Mindestinformationen anzuzeigender Ereignisse** können Sie den niedrigsten Schweregrad der anzuzeigenden Warnungen und Hinweise wählen.

- **Diagnose** - Alle Meldungen höherer Stufen und alle sonstigen Informationen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.
- **Informationen** - Meldungen wie erfolgreiche Updates und alle Meldungen höherer Stufen werden protokolliert.
- **Warnungen** - Kritische Fehler und Warnungen werden protokolliert.
- **Fehler** - Fehler wie *„Fehler beim Herunterladen der Datei“* und kritische Fehler werden aufgezeichnet.
- **Kritische Warnungen** - Nur kritische Warnungen (z. B. bei einem Fehler beim Start des Virenschutz-Moduls, beim Ausführen der Personal Firewallusw.) werden protokolliert.

Der letzte Eintrag in diesem Bereich gibt Ihnen die Möglichkeit, die Ausgabe für Meldungen in einer Mehrbenutzerumgebung zu konfigurieren. Mit dem Feld **Auf Mehrbenutzersystemen Hinweise auf dem Bildschirm des folgenden Benutzers ausgeben** können Sie festlegen, bei welchem Benutzer Warnungen und Hinweise angezeigt werden, wenn mehrere Benutzer gleichzeitig angemeldet sind. Üblicherweise wird hier der System- oder Netzwerkadministrator gewählt. Besonders sinnvoll ist diese Option bei Terminalservern, vorausgesetzt alle Systemmeldungen werden an den Administrator gesendet.

4.7.3 Versteckte Hinweisfenster

Wenn die Option **Dieses Fenster nicht mehr anzeigen** für ein Hinweisfenster (eine Warnung) aktiviert wurde, das schon einmal angezeigt wurde, wird dieses in der Liste der versteckten Hinweisfenster angezeigt. Aktionen, die nunmehr automatisch ausgeführt werden, werden in der Spalte mit dem Titel **Bestätigen** angezeigt.

Anzeigen - Zeigt eine Vorschau aller Hinweisfenster an, die derzeit nicht angezeigt werden und für die eine automatische Aktion konfiguriert wurde.

Entfernen - Entfernen von **Versteckten Hinweisfenstern** aus der Liste. Alle aus der Liste entfernten Hinweisfenster werden wieder angezeigt.

4.7.4 Einstellungen für den Zugriff

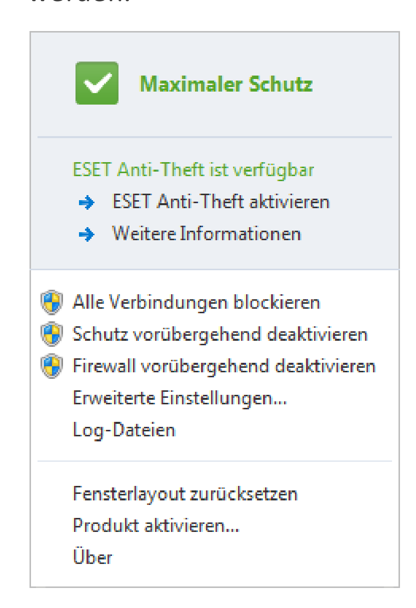
Die Einstellungen von ESET Smart Security sind ein wichtiger Bestandteil Ihrer Sicherheitsrichtlinien. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Um die Programmeinstellungen mit einem Passwort zu schützen, klicken Sie im Hauptmenü auf **Einstellungen** > **Erweiterte Einstellungen** > **Benutzeroberfläche** > **Einstellungen für den Zugriff**. Wählen Sie die Option **Einstellungen mit Passwort schützen** und klicken Sie auf **Passwort festlegen**. Beachten Sie die Groß-/Kleinschreibung des Passworts.

Volle Administratorrechte für eingeschränkte Administratorkonten anfordern - Aktivieren Sie dies, damit Benutzer ohne Administratorrechte zur Eingabe eines Administratorbenutzernamens und -passworts aufgefordert werden, wenn sie bestimmte Systemeinstellungen ändern möchten (ähnlich der Benutzerkontensteuerung/UAC in Windows Vista und Windows 7). Dazu gehören das Deaktivieren von Schutzmodulen oder das Abschalten der Firewall. Auf Windows XP-Systemen, auf denen die Benutzerkontensteuerung (UAC) nicht ausgeführt wird, ist die Option **Administratorrechte bei Bedarf anfordern (Systeme ohne UAC-Support)** verfügbar.

Dialogfenster für Dauer anzeigen, wenn Schutz vorübergehend deaktiviert wird - Wenn dies aktiviert ist, wird jedes Mal, wenn der Benutzer den Schutz über das Programmmenü oder unter **ESET Smart Security** > **Einstellungen** vorübergehend deaktiviert, ein Dialogfenster mit der verbleibenden Deaktivierungsdauer angezeigt.

4.7.5 Programmmenü

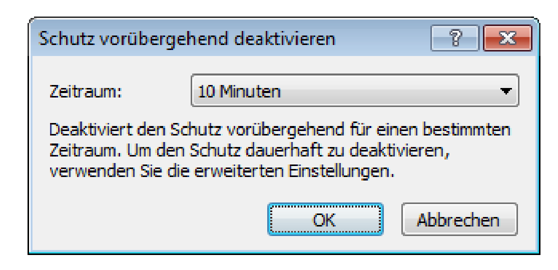
Über das Menü des Hauptprogramms können einige der wichtigsten Einstellungen und Funktionen aufgerufen werden.



Häufig verwendet - Zeigt die am häufigsten verwendeten Komponenten von ESET Smart Security an. Auf diese haben Sie direkt aus dem Programmmenü Zugriff.

Schutz vorübergehend deaktivieren - Zeigt ein Dialogfenster an, in dem Sie bestätigen müssen, dass der Viren- und Spyware-Schutz deaktiviert wird, der Dateivorgänge sowie die Internet- und E-Mail-Kommunikation überwacht und so Ihr System vor Angriffen schützt. Aktivieren Sie **Nicht erneut nachfragen**, um diese Meldung in Zukunft nicht mehr anzuzeigen.

Über das Dropdown-Menü **Zeitraum** können Sie festlegen, wie lange der Viren- und Spyware-Schutz deaktiviert sein soll.



Alle Verbindungen blockieren - Die Personal Firewall blockiert den gesamten eingehenden und ausgehenden

Netzwerk- und Internet-Datenverkehr.

Firewall vorübergehend deaktivieren - Die Firewall ist vorübergehend inaktiv. Weitere Informationen finden Sie im Kapitel Systemintegration der Personal Firewall.

Erweiterte Einstellungen - Öffnet die Baumstruktur **Erweiterte Einstellungen**. Alternativ können die erweiterten Einstellungen auch mit der Taste F5 oder unter **Einstellungen** > **Erweiterte Einstellungen** angezeigt werden.

Log-Dateien - Log-Dateien enthalten Informationen zu wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen.

Fensterlayout zurücksetzen - Stellt die standardmäßige Fenstergröße von ESET Smart Security und deren Standardposition auf dem Bildschirm wieder her.

Produkt aktivieren... - Wählen Sie diese Option aus, wenn Sie Ihr ESET-Sicherheitsprodukt noch nicht aktiviert haben, oder um die Produktaktivierungsdaten nach einer Lizenzverlängerung erneut einzugeben.

Über - Bietet Systeminformationen zur installierten Version von ESET Smart Security und zu den installierten Programmmodulen. Hier finden Sie außerdem das Lizenzablaufdatum und Informationen zum Betriebssystem und zu den Systemressourcen.

4.7.6 Kontextmenü

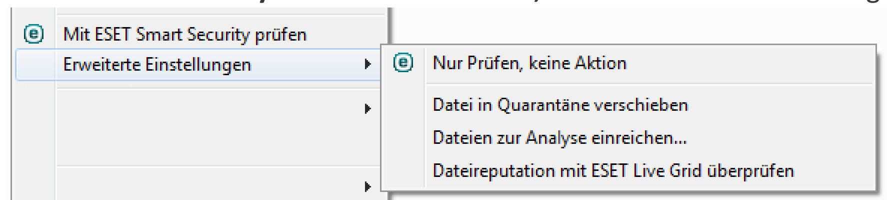
Das Kontextmenü wird angezeigt, wenn Sie mit der rechten Maustaste auf ein Element klicken. Das Menü enthält alle Optionen, die auf das Objekt angewendet werden können.

Bestimmte Steuerungselemente von ESET Smart Security können in das Kontextmenü integriert werden. Weitere Einstellungsoptionen für diese Funktion sind unter „Erweiterte Einstellungen“ im Bereich **Benutzeroberfläche** > **Kontextmenü** verfügbar.

In Kontextmenü integrieren - ESET Smart Security kann in das Kontextmenü integriert werden.

Folgende Optionen stehen in der Liste **Menütyp** zur Verfügung:

- **Voll (zuerst prüfen)** - Aktiviert alle Optionen für das Kontextmenü; das Hauptmenü zeigt die Option **Mit ESET Smart Security prüfen, ohne zu säubern** als Erstes und **Scan and clean** (Prüfen und säubern) als untergeordnete Option.
- **Voll (zuerst säubern)** - Aktiviert alle Optionen für das Kontextmenü; das Hauptmenü zeigt die Option **Prüfen mit ESET Smart Security** als Erstes und **Prüfen, ohne zu säubern** als untergeordnete Option.



- **Nur prüfen** - Im Kontextmenü wird nur die Option **Mit ESET Smart Security prüfen, ohne zu säubern** angezeigt.
- **Nur säubern** - Im Kontextmenü erscheint nur die Option **Prüfen mit ESET Smart Security**.

5. Fortgeschrittene Benutzer

5.1 Profilmanager

An zwei Stellen von ESET Smart Security wird der Profilmanager verwendet: in den Bereichen **On-Demand-Prüfung** und **Update**.

Computer prüfen

Ihre bevorzugten Einstellungen können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

Um ein neues Profil zu erstellen, öffnen Sie das Fenster mit den erweiterten Einstellungen (F5) und klicken Sie auf **Computer** > **Viren- und Spyware-Schutz** > **On-Demand-Prüfung** > **Profile...**. Im Fenster **Konfigurationsprofile** befindet sich das Dropdown-Menü **Ausgewähltes Profil** mit den vorhandenen Prüfprofilen und der Option zum Erstellen eines neuen Profils. Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt Einstellungen für ThreatSense. So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Beispiel: Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Smart-Prüfung eignet sich in gewissem Maße, aber Sie möchten nicht die laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option **Immer versuchen, automatisch zu entfernen** anwenden. Klicken Sie im Fenster **Konfigurationsprofile** auf **Hinzufügen...**. Geben Sie den Namen des neuen Profils im Feld **Profilname** ein und wählen Sie im Dropdown-Menü **Einstellungen kopieren von Profil** die Option **Smart-Prüfung**. Passen Sie anschließend die übrigen Parameter Ihren eigenen Erfordernissen an und speichern Sie Ihr neues Profil.

Update

Mit dem Profil-Editor unter „Einstellungen für Updates“ können Benutzer neue Update-Profile erstellen. Das Erstellen und Verwenden eigener benutzerdefinierter Profile (d. h. anderer Profile als das standardmäßige **Mein Profil**) ist nur sinnvoll, wenn Ihr Computer auf mehrere Verbindungsarten zurückgreifen muss, um eine Verbindung zu den Update-Servern herzustellen.

Nehmen wir als Beispiel einen Laptop, dessen Updates normalerweise über einen lokalen Server (einen sogenannten Mirror) im lokalen Netzwerk erfolgen, der aber seine Updates direkt von den ESET-Update-Servern bezieht, wenn keine Verbindung zum lokalen Netzwerk hergestellt werden kann (z. B. auf einer Geschäftsreise). Dieser Laptop kann zwei Profile haben: das erste Profil für die Verbindung zum lokalen Server, das zweite Profil für die Verbindung zu den ESET-Servern. Sobald diese Profile eingerichtet sind, wählen Sie **Tools** > **Taskplaner** und bearbeiten Sie die Update-Task-Einstellungen. Legen Sie eines der Profile als primäres Profil fest, das andere als sekundäres Profil.

Ausgewähltes Profil - Das momentan verwendete Update-Profil. Um es zu ändern, wählen Sie ein Profil aus dem Dropdown-Menü aus.

Hinzufügen - Erstellen neuer Updateprofile.

Im unteren Teil des Fensters sind die vorhandenen Profile aufgelistet.

5.2 Tastaturbefehle

Für die Arbeit mit ESET Smart Security stehen Ihnen die folgenden Tastaturbefehle zur Verfügung:

Strg+G	deaktiviert die grafische Benutzeroberfläche des Produkts
Strg+I	öffnet die Seite „ESET SysInspector“
Strg+L	öffnet die Seite Log-Dateien
Strg+S	öffnet die Seite Taskplaner
Strg+Q	öffnet die Seite Quarantäne
Strg+U	öffnet die Einrichtung eines Benutzerkontos und Passworts

Strg+R	stellt die standardmäßige Fenstergröße und die standardmäßige Fensterposition auf dem Bildschirm wieder her.

Zur besseren Navigation in Ihrem ESET-Produkt stehen die folgenden Tastaturbefehle zur Verfügung:

F1	öffnet die Hilfeseiten
F5	öffnet die erweiterten Einstellungen
Pfeiltasten nach oben/ unten	Navigation in der Software durch Elemente
*	erweitert den Knoten unter „Erweiterte Einstellungen“
-	reduziert den Knoten unter „Erweiterte Einstellungen“
TAB	bewegt den Cursor in einem Fenster
Esc	schließt das aktive Dialogfenster

5.3 Diagnose

Mit der Diagnose können Speicherabbilddateien von ESET-Prozessen erstellt werden (z. B. *ekrn*). Im Falle eines Absturzes einer Anwendung wird eine Speicherabbilddatei erstellt. Diese kann Entwicklern helfen, Fehler im Code zu finden und verschiedene Probleme von ESET Smart Security zu lösen. Es stehen zwei Typen von Speicherabbilddateien zur Verfügung:

- **Vollständiges Speicherabbild** - Zeichnet den gesamten Inhalt des Arbeitsspeichers auf, wenn die Anwendung unerwartet beendet wird. Ein vollständiges Speicherabbild kann auch Daten von Prozessen enthalten, die ausgeführt wurden, als das Speicherabbild geschrieben wurde.
- **Kleines Speicherabbild** - Protokolliert die kleinste Menge an Daten, die helfen könnten, die Ursache für den Absturz der Anwendung herauszufinden. Dieser Dateityp ist eher zu empfehlen, wenn der Speicherplatz begrenzt ist. Da jedoch die enthaltene Datenmenge ebenfalls begrenzt ist, könnten Fehler, die nicht direkt von dem Thread ausgelöst wurden, der zum Absturzzeitpunkt ausgeführt wurde, bei einer Dateianalyse unentdeckt bleiben.
- Wählen Sie **Kein Speicherabbild erstellen** (Standardeinstellung), um diese Funktion zu deaktivieren.

Zielverzeichnis - Verzeichnis, in dem die Speicherabbilddatei während des Absturzes erstellt wird. Klicken Sie auf **Ordner öffnen**, um dieses Verzeichnis in einem neuen Fenster von *Windows Explorer* zu öffnen.

5.4 Einstellungen importieren/exportieren

Über das Menü **Einstellungen** können Sie die XML-Datei mit Ihrer benutzerdefinierten Konfiguration von ESET Smart Security importieren und exportieren.

Das Importieren und Exportieren der Konfigurationsdatei ist hilfreich, wenn Sie zur späteren Verwendung eine Sicherung der aktuellen Konfiguration von ESET Smart Security erstellen möchten. Die Exportfunktion bietet sich auch für Benutzer an, die ihre bevorzugte Konfiguration auf mehreren Systemen verwenden möchten. Um die Einstellungen zu übernehmen, wird einfach eine Datei mit der Endung *.xml* importiert.

Die Schritte zum Importieren einer Konfiguration sind sehr einfach. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Einstellungen importieren/exportieren**, und wählen Sie die Option **Einstellungen importieren**. Geben Sie den Namen der Konfigurationsdatei ein oder klicken Sie auf **Durchsuchen**, um die Konfigurationsdatei zu suchen, die Sie importieren möchten.

Der Export einer Konfiguration verläuft sehr ähnlich. Klicken Sie im Hauptprogrammfenster auf **Einstellungen** > **Einstellungen importieren/exportieren**. Wählen Sie **Einstellungen exportieren** und geben Sie den Namen der Konfigurationsdatei (z. B. *export.xml*) ein. Suchen Sie mithilfe des Browsers einen Speicherort auf Ihrem Computer aus, an dem Sie die Konfigurationsdatei speichern möchten.

Hinweis: Beim Exportieren der Einstellungen kann ein Fehler auftreten, wenn Sie über unzureichende Berechtigungen für das angegebene Verzeichnis verfügen.



5.5 Erkennen des Leerlaufs

Die Erkennung des Ruhezustands kann in **Erweiterte Einstellungen** unter **Tools** > **Erkennen des Leerlaufs** konfiguriert werden. Unter diesen Einstellungen können folgende Auslöser für das Prüfen im Leerlaufbetrieb festgelegt werden:

- Aktivierung des Bildschirmschoners
- Sperren des Computers
- Abmelden eines Benutzers

Aktivieren bzw. deaktivieren Sie die Auslöser für die Prüfung im Ruhezustand über die entsprechenden Kontrollkästchen.

5.6 ESET SysInspector

5.6.1 Einführung in ESET SysInspector

ESET SysInspector ist eine Anwendung, die den Computer gründlich durchsucht und die gesammelten Daten ausführlich anzeigt. Informationen wie installierte Treiber und Anwendungen, Netzwerkverbindungen und wichtige Einträge in der Registrierung helfen Ihnen, verdächtiges Systemverhalten, sei es auf Grund von Software- oder Hardwareinkompatibilität oder einer Infektion mit Schadsoftware, zu untersuchen.

Sie können auf zwei Arten auf ESET SysInspector zugreifen: über die in ESET Security-Produkte integrierte Version oder indem Sie die eigenständige Version (SysInspector.exe) kostenlos von der ESET-Website herunterladen. Die Funktionen und Steuerelemente beider Programmversionen sind identisch. Die Versionen unterscheiden sich nur in der Ausgabe der Informationen. Sowohl mit der eigenständigen als auch der integrierten Version können Snapshots des Systems in einer *.xml*-Datei ausgegeben und auf einem Datenträger gespeichert werden. Mit der integrierten Version können Sie Systemsnapshots außerdem direkt unter **Tools** > **ESET SysInspector** speichern (Ausnahme: ESET Remote Administrator). Weitere Informationen finden Sie im Abschnitt ESET SysInspector als Teil von ESET Smart Security.

Bitte gedulden Sie sich ein wenig, während ESET SysInspector Ihren Computer prüft. Je nach aktueller Hardware-Konfiguration, Betriebssystem und Anzahl der installierten Anwendungen kann die Prüfung zwischen 10 Sekunden und einigen Minuten dauern.

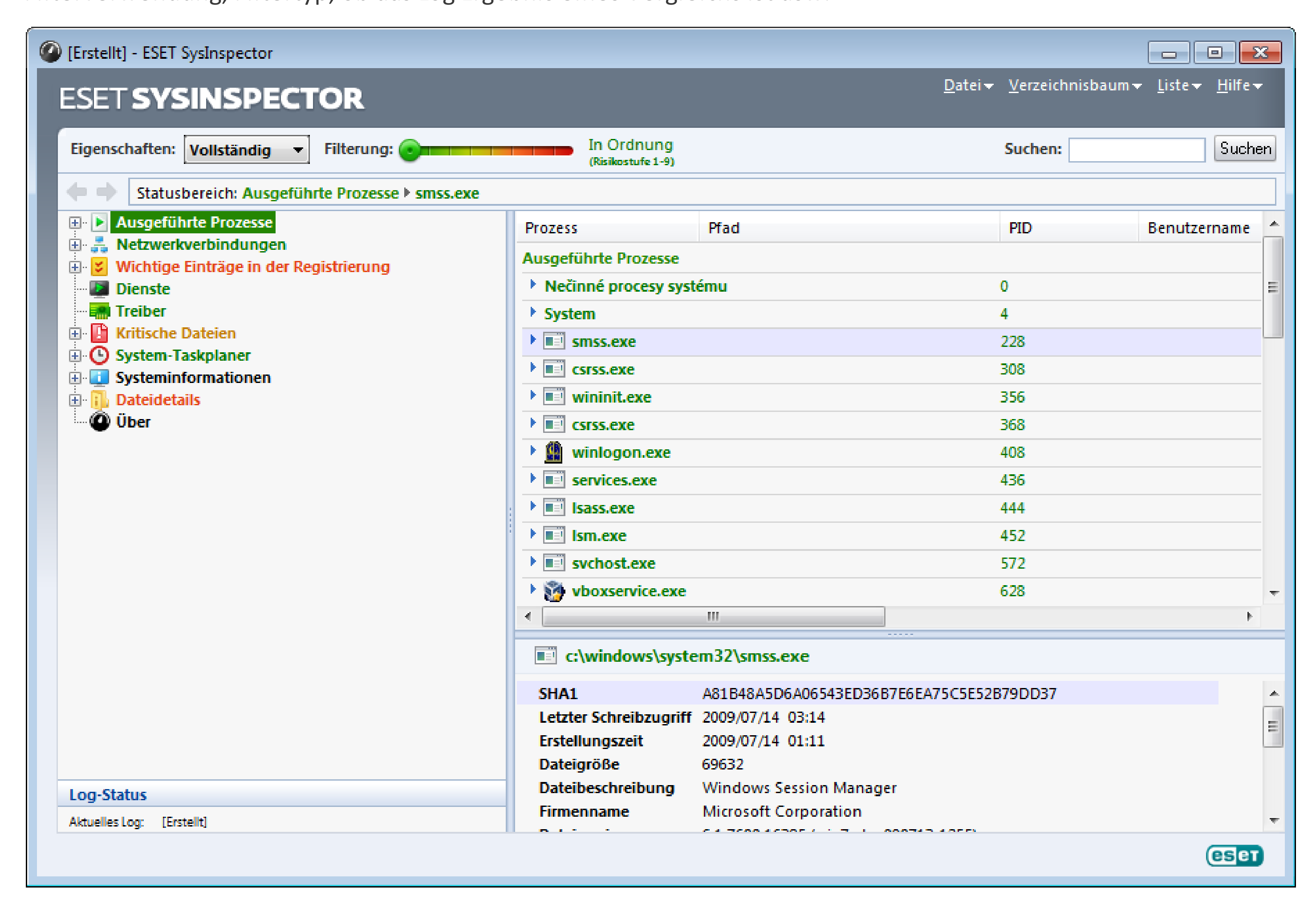
5.6.1.1 Starten von ESET SysInspector

Zum Starten von ESET SysInspector führen Sie einfach die von der ESET-Website heruntergeladene Programmdatei *SysInspector.exe* aus. Wenn bereits ein ESET Security-Produkt installiert ist, können Sie ESET SysInspector direkt aus dem Startmenü starten (**Programme** > **ESET** > **ESET Smart Security**).

Warten Sie, während die Anwendung das System überprüft. Dies kann einige Minuten in Anspruch nehmen.

5.6.2 Benutzeroberfläche und Verwenden der Anwendung

Zur besseren Übersicht ist das Hauptprogrammfenster in vier größere Bereiche unterteilt: die Steuerelemente des Programms oben, das Navigationsfenster links, das Beschreibungsfenster rechts und das Detailfenster unten im Hauptfenster. Im Bereich „Log-Status“ werden die grundlegenden Parameter eines Logs aufgeführt: Filterverwendung, Filtertyp, ob das Log Ergebnis eines Vergleichs ist usw.



5.6.2.1 Steuerelemente des Programms

Dieser Abschnitt beschreibt die Menüs und sonstigen Bedienelemente in ESET SysInspector.

Datei

Über das Menü **Datei** können Sie die aktuellen Systeminformationen zur späteren Untersuchung speichern oder ein zuvor gespeichertes Log wieder öffnen. Falls ein Log weitergegeben werden soll, sollten Sie es über die Funktion **Zum Senden geeignet** erstellen. Sicherheitsrelevante Daten (Name und Berechtigungen des aktuellen Benutzers, Computername, Domänenname, Umgebungsvariablen usw.) werden dann nicht in das Log aufgenommen.

HINWEIS: Gespeicherte ESET SysInspector-Logs können Sie schnell wieder öffnen, indem Sie sie auf das Hauptprogrammfenster ziehen und dort ablegen.

Verzeichnisbaum

Hiermit können Sie alle Knoten erweitern oder schließen sowie die ausgewählten Bereiche in ein Dienste-Skript

exportieren.

Liste

Dieses Menü enthält Funktionen zur einfacheren Navigation im Programm sowie eine Reihe von Zusatzfunktionen, etwa für die Online-Informationssuche.

Hilfe

Über dieses Menü finden Sie Informationen zur Anwendung und ihren Funktionen.

Eigenschaften

Dieses Menü beeinflusst die Informationen, die im Hauptprogrammfenster dargestellt werden und vereinfacht somit ihre Verwendung. Im Modus „Einfach" haben Sie Zugang zu Informationen, die Hilfestellung bei gewöhnlichen Problemen im System liefern. Im Modus „Mittel" sehen Sie weniger häufig benötigte Informationen. Im Modus „Vollständig" zeigt ESET SysInspector alle verfügbaren Informationen an, sodass Sie auch sehr spezielle Probleme beheben können.

Filterung

Mit der Filterfunktion können Sie schnell verdächtige Dateien oder Registrierungseinträge auf Ihrem System finden. Durch Verschieben des Schiebereglers legen Sie fest, ab welcher Risikostufe Objekte angezeigt werden. Befindet sich der Schieberegler ganz links (Risikostufe 1), werden alle Einträge angezeigt. Steht der Schieberegler hingegen weiter rechts, werden alle Objekte unterhalb der eingestellten Risikostufe ausgeblendet, sodass Sie nur die Objekte ab einer bestimmten Risikostufe sehen. Steht der Schieberegler ganz rechts, zeigt das Programm nur die als schädlich bekannten Einträge an.

Alle Objekte der Risikostufen 6 bis 9 stellen unter Umständen ein Sicherheitsrisiko dar. Falls solche Objekte auf Ihrem System gefunden werden und Sie keine ESET Security-Lösung einsetzen, empfiehlt sich eine Überprüfung Ihres Systems mit dem kostenlosen ESET Online Scanner.

HINWEIS: Die Risikostufe eines Eintrags können Sie leicht erkennen, indem Sie dessen Farbe mit der Farbe auf der Risikostufenskala vergleichen.

Vergleichen

Beim Vergleich zweier Log-Dateien können Sie angeben, ob alle Elemente, nur hinzugefügte Elemente, nur entfernte Elemente oder nur ersetzte Elemente angezeigt werden sollen.

Suchen

Mit der Suche können Sie ein bestimmtes Objekt schnell über seinen Namen (oder einen Teil des Namens) finden. Die Suchergebnisse werden im Beschreibungsfenster angezeigt.

Zurück

Über die Schaltflächen mit den Pfeilen nach links und rechts können Sie zwischen den bisherigen Anzeigeinhalten des Beschreibungsbereichs wechseln. Anstatt auf „Vor" und „Zurück" zu klicken, können Sie auch die Leertaste bzw. Rücktaste (Backspace) verwenden.

Statusbereich

Hier sehen Sie, welcher Knoten im Navigationsbereich gerade ausgewählt ist.

Wichtig: Rot hervorgehobene Objekte sind unbekannt und werden daher als potenziell gefährlich markiert. Falls ein Eintrag rot gefärbt ist, heißt das jedoch nicht zwingend, dass Sie die Datei löschen können. Stellen Sie vor dem Löschen sicher, dass die Dateien wirklich gefährlich oder unnötig sind.

5.6.2.2 Navigation in ESET SysInspector

In ESET SysInspector gliedern sich die unterschiedlichen Systeminformationen in eine Reihe von Hauptabschnitten, die so genannten „Knoten“. Falls zusätzliche Informationen verfügbar sind, erreichen Sie diese, indem Sie einen Knoten um seine Unterknoten erweitern. Um einen Knoten zu öffnen oder zu reduzieren, doppelklicken Sie auf den Knotennamen oder klicken Sie neben dem Knotennamen auf ⊞ bzw. ⊟. Soweit vorhanden, werden im Beschreibungsbereich Detailinhalte zum gerade im Navigationsbereich ausgewählten Knoten angezeigt. Diese Einträge im Beschreibungsbereich können Sie dann wiederum auswählen, um (soweit vorhanden) im Detailbereich weitere Detailinformationen dazu anzuzeigen.

Im Folgenden sind die Hauptknoten im Navigationsbereich sowie die dazugehörigen Informationen im Beschreibungs- und Detailbereich beschrieben.

Ausgeführte Prozesse

Dieser Knoten enthält Informationen zu den Anwendungen und Prozessen, die zum Zeitpunkt der Log-Erstellung ausgeführt wurden. Das Beschreibungsfenster zeigt weitere Details zu jedem Prozess, etwa die verwendeten dynamischen Bibliotheken samt Speicherort, den Namen des Programmherstellers und die Risikostufe der Dateien.

Wenn Sie einen Eintrag im Beschreibungsfenster auswählen, erscheinen im Detailfenster weitere Informationen wie z. B. die Größe oder der Hashwert der betreffenden Datei.

HINWEIS: Ein Betriebssystem enthält verschiedene durchgängig laufende Kernelkomponenten, die grundlegende und wichtige Funktionen für andere Benutzeranwendungen bereitstellen. In bestimmten Fällen wird für solche Prozesse in ESET SysInspector ein Dateipfad angezeigt, der mit \??\ beginnt. Diese Symbole stellen eine vor dem Start liegende Optimierung für derartige Prozesse dar. Sie sind für das System ungefährlich.

Netzwerkverbindungen

Wenn Sie im Navigationsbereich ein Protokoll (TCP oder UDP) auswählen, erscheint im Beschreibungsbereich eine Liste der Prozesse und Anwendungen, die über das betreffende Protokoll im Netzwerk kommunizieren, samt der jeweiligen Remoteadresse. Außerdem können Sie hier die IP-Adressen der DNS-Server überprüfen.

Wenn Sie einen Eintrag im Beschreibungsfenster auswählen, erscheinen im Detailfenster weitere Informationen wie z. B. die Größe oder der Hashwert der betreffenden Datei.

Wichtige Einträge in der Registrierung

Hier finden Sie eine Liste ausgewählter Registrierungseinträge, die oft im Zusammenhang mit Systemproblemen stehen. Dies betrifft beispielsweise die Registrierungseinträge für Autostart-Programme, Browser-Hilfsobjekte (BHO) usw.

Im Beschreibungsbereich werden die mit dem jeweiligen Registrierungseintrag verbundenen Dateien angezeigt. Das Detailfenster zeigt zusätzliche Informationen an.

Dienste

Bei diesem Knoten enthält der Beschreibungsbereich eine Liste der Dateien, die als Windows-Dienste registriert sind. Das Detailfenster informiert über spezifische Details und darüber, auf welche Art ein Dienst gestartet wird.

Treiber

Dieser Knoten enthält eine Liste der im System installierten Treiber.

Kritische Dateien

Unter diesem Knoten können Sie sich im Beschreibungsbereich den Inhalt wichtiger Konfigurationsdateien von Microsoft Windows anzeigen lassen.

System-Taskplaner

Enthält eine Liste der Tasks, die der Windows-Taskplaner (in neueren Windows-Versionen „Aufgabenplanung“ genannt) zu einem festgelegten Zeitpunkt/in festgelegten Intervallen auslöst.

Systeminformationen

Hier finden Sie ausführliche Informationen zu Hardware und Software, den gesetzten Umgebungsvariablen, den Benutzerberechtigungen und den Systemereignis-Logs.

Dateidetails

Dieser Knoten enthält eine Liste der wichtigen Systemdateien sowie der Dateien im Ordner „Programme“. Zusätzliche Informationen speziell für diese Dateien werden im Beschreibungs- und Detailfenster angezeigt.

Über

Angaben zur Version von ESET SysInspector und eine Liste der Programmmodule.

5.6.2.2.1 Tastaturbefehle

Für die Arbeit mit ESET SysInspector stehen Ihnen die folgenden Tastaturbefehle zur Verfügung:

Datei

Strg+O	bestehendes Log öffnen
Strg+S	erstelltes Log speichern

Erstellen

Strg+G	erstellt einen Snapshot des Computerstatus
Strg+H	erstellt einen Snapshot des Computerstatus, der auch sicherheitsrelevante Informationen im Log enthalten kann

Filterung der Elemente

1, O	in Ordnung, Einträge der Risikostufen 1-9 werden angezeigt
2	in Ordnung, Einträge der Risikostufen 2-9 werden angezeigt
3	in Ordnung, Einträge der Risikostufen 3-9 werden angezeigt
4, U	unbekannt, Einträge der Risikostufen 4-9 werden angezeigt
5	unbekannt, Einträge der Risikostufen 5-9 werden angezeigt
6	unbekannt, Einträge der Risikostufen 6-9 werden angezeigt
7, B	risikoreich, Einträge der Risikostufen 7-9 werden angezeigt
8	risikoreich, Einträge der Risikostufen 8-9 werden angezeigt
9	risikoreich, Einträge der Risikostufe 9 werden angezeigt
-	verringert Risikostufe
+	erhöht Risikostufe
Strg+9	Filtermodus, gleiche oder höhere Stufe
Strg+0	Filtermodus, nur gleiche Stufe

Ansicht

Strg+5	Anzeige nach Anbieter, alle Anbieter
Strg+6	Anzeige nach Anbieter, nur Microsoft
Strg+7	Anzeige nach Anbieter, alle anderen Anbieter
Strg+3	zeigt vollen Detailmodus an
Strg+2	zeigt mittleren Detailmodus an
Strg+1	einfache Darstellung
Rücktaste	geht einen Schritt zurück
Leertaste	geht einen Schritt vor
Strg+W	erweitert die Baumstruktur
Strg+Q	reduziert die Baumstruktur

Sonstige Steuerelemente

Strg+T	kehrt nach der Auswahl von Suchergebnissen zum Ursprung des Eintrags zurück
Strg+P	zeigt grundlegende Informationen zu einem Eintrag an

Strg+A	zeigt alle Informationen zu einem Eintrag an
Strg+C	kopiert die Baumstruktur des aktuellen Eintrags
Strg+X	kopiert Einträge
Strg+B	sucht im Internet nach Informationen zu den ausgewählten Dateien
Strg+L	öffnet den Ordner, in dem sich die ausgewählte Datei befindet
Strg+R	öffnet den dazugehörigen Eintrag im Registrierungs-Editor
Strg+Z	kopiert den Pfad in eine Datei (falls der Eintrag mit einer Datei zusammenhängt)
Strg+F	zum Suchfeld wechseln
Strg+D	schließt die Suchergebnisse
Strg+E	startet ein Dienste-Skript

Vergleichen

Strg+Alt+O	öffnet das Original-/Vergleichs-Log
Strg+Alt+R	bricht das Vergleichen ab
Strg+Alt+1	zeigt alle Einträge an
Strg+Alt+2	zeigt nur hinzugekommene Einträge an, das Log listet die aktuellen Einträge auf
Strg+Alt+3	zeigt nur entfernte Einträge an, das Log listet die Einträge des vorherigen Logs auf
Strg+Alt+4	zeigt nur ersetzte Einträge an (Dateien eingeschlossen)
Strg+Alt+5	führt lediglich Unterschiede zwischen den Logs auf
Strg+Alt+C	Vergleich anzeigen
Strg+Alt+N	zeigt das aktuelle Log an
Strg+Alt+P	öffnet das vorherige Log

Allgemein

F1	ruft die Hilfe auf
Alt+F4	schließt das Programm
Alt+Umschalt+F4	schließt das Programm ohne Nachfrage
Strg+I	Log-Statistiken

5.6.2.3 Vergleichsfunktion

Mit der „Vergleichen“-Funktion ist es möglich, zwei bestehende Log-Dateien miteinander zu vergleichen. Auf diese Weise erlangen Sie Informationen, die aus den beiden einzelnen Log-Dateien für sich genommen nicht hervorgehen. Diese Funktion ist geeignet, um Änderungen am System zu erkennen, und hilft so, Schadprogramme zu entdecken.

Nach dem Start erzeugt die Anwendung ein neues Log, das in einem neuen Fenster angezeigt wird. Um das Log zu speichern, klicken Sie auf **Datei** > **Log speichern**. Gespeicherte Log-Dateien können Sie später wieder öffnen, um sie einzusehen. Ein bestehendes Log öffnen Sie über **Datei** > **Log öffnen**. Im Hauptfenster von ESET SysInspector wird immer nur jeweils ein Log angezeigt.

Die Vergleichsfunktion hat den Vorteil, dass Sie sich eine aktive und eine gespeicherte Log-Datei anzeigen lassen können. Hierzu klicken Sie auf **Datei** > **Logs vergleichen** und wählen dann **Datei auswählen**. Das gewählte Log wird mit dem gerade aktiven im Hauptprogrammfenster verglichen. Das Vergleichs-Log führt lediglich Unterschiede zwischen diesen beiden Logs auf.

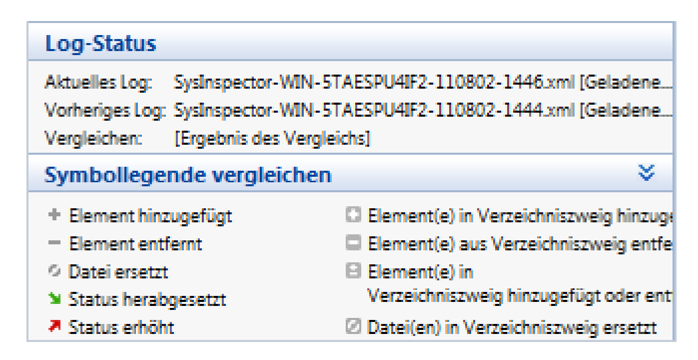
HINWEIS: Wenn Sie nach dem Vergleich zweier Logs auf **Datei** > **Log speichern** klicken und das Ergebnis als ZIP-Datei speichern, werden beide Log-Dateien gespeichert. Wenn Sie die so entstandene Datei später öffnen, werden die enthaltenen Logs automatisch verglichen.

Neben den einzelnen Einträgen erscheinen Symbole, die angeben, um was für eine Art von Unterschied es sich handelt.

Beschreibung aller Symbole, die neben den Einträgen angezeigt werden können:

- Neuer Wert, nicht im vorherigen Log enthalten
- Betreffender Zweig der Baumstruktur enthält neue Werte
- Gelöschter Wert, nur im vorherigen Log enthalten
- Betreffender Zweig der Baumstruktur enthält gelöschte Werte
- Wert/Datei wurde geändert
- Betreffender Zweig der Baumstruktur enthält geänderte Werte/Dateien
- Risiko ist gesunken (war im vorherigen Log höher)
- Risiko ist gestiegen (war im vorherigen Log niedriger)

Der Erklärungsbereich in der linken unteren Ecke beschreibt alle Symbole und zeigt auch die Namen der Log-Dateien an, die verglichen werden.



Jedes Vergleichs-Log kann als Datei gespeichert und später wieder geöffnet werden.

Beispiel

Erstellen und speichern Sie ein Log, das die ursprünglichen Informationen über das System enthält, als vorher.xml. Nachdem Sie Änderungen am System vorgenommen haben, öffnen Sie ESET SysInspector und erstellen Sie ein neues Log. Speichern Sie dieses unter dem Namen *neu.xml*.

Um die Unterschiede zwischen diesen beiden Logs zu sehen, klicken Sie auf **Datei** > **Logs vergleichen**. Das Programm erstellt nun ein Vergleichs-Log, das die Unterschiede beider Log-Dateien anzeigt.

Mithilfe des folgenden Befehls in der Kommandozeile kann das gleiche Resultat erzielt werden:

SysInspector.exe aktuell.xml vorher.xml

5.6.3 Kommandozeilenparameter

Mit ESET SysInspector können Sie auch von der Kommandozeile aus Berichte erzeugen. Hierzu stehen die folgenden Parameter zur Verfügung:

/gen	Log direkt über die Kommandozeile erstellen, ohne die Benutzeroberfläche zu starten
/privacy	Log ohne vertrauliche Daten erstellen
/zip	Log in komprimiertem Zip-Archiv speichern
/silent	Fortschrittsanzeige unterdrücken, wenn Log von der Kommandozeile aus erstellt wird
/blank	ESET-SysInspector starten, ohne Log zu erstellen/laden

Beispiele

Verwendung:
```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Spezielles Log direkt im Browser öffnen: *SysInspector.exe .\clientlog.xml*
Log über die Kommandozeile erstellen: *SysInspector.exe /gen=.\mynewlog.xml*
Log ohne vertrauliche Informationen direkt in einer komprimierten Datei erstellen: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Zwei Log-Dateien vergleichen und Unterschiede durchsuchen: *SysInspector.exe new.xml old.xml*

HINWEIS: Datei- und Ordnernamen mit Leerzeichen sollten in Hochkommata gesetzt werden.

5.6.4 Dienste-Skript

Ein Dienste-Skript ist ein Hilfsmittel für Benutzer von ESET SysInspector zur einfachen Entfernung unerwünschter Objekte aus dem System.

Das Dienste-Skript ermöglicht den Export des gesamten ESET SysInspector-Logs oder ausgewählten Teilen davon. Nach dem Export können Sie unerwünschte Objekte zum Löschen markieren. Anschließend können Sie das so bearbeitete Log ausführen, um die markierten Objekte zu löschen.

Das Dienste-Skript ist für fortgeschrittene Benutzer geeignet, die bereits Erfahrung mit der Diagnose von Systemproblemen haben. Unqualifizierte Änderungen können das Betriebssystem beschädigen.

Beispiel

Wenn Sie vermuten, dass Ihr Computer mit einem Virus infiziert ist, den Ihr Antivirusprogramm nicht erkennt, gehen Sie wie folgt vor:

1. Führen Sie ESET SysInspector aus, um einen neuen System-Snapshot zu erstellen.
2. Wählen Sie den ersten Menüpunkt im Bereich auf der linken Seite (in der Baumstruktur). Halten Sie die Umschalttaste gedrückt und wählen Sie den letzten Menüpunkt, um alle Menüpunkte zu markieren.
3. Klicken Sie mit der rechten Maustaste auf die ausgewählten Objekte und wählen Sie **Ausgewählte Bereiche in das Entfernen-Skript exportieren** aus.
4. Die ausgewählten Objekte werden in ein neues Log exportiert.
5. Es folgt der wichtigste Schritt des gesamten Vorgangs: Öffnen Sie das neue Log und ändern Sie das Zeichen „-“ vor allen Objekten, die gelöscht werden sollen, auf „+“. Stellen Sie sicher, dass Sie keine wichtige Betriebssystemdateien oder -objekte markieren.
6. Öffnen Sie ESET SysInspector, klicken Sie auf **Datei** > **Dienste-Skript ausführen** und geben Sie den Pfad zum Skript ein.
7. Klicken Sie auf **OK**, um das Skript auszuführen.

5.6.4.1 Erstellen eines Dienste-Skripts

Um ein Skript zu erstellen, klicken Sie im ESET SysInspector-Hauptfenster mit der rechten Maustaste auf ein beliebiges Element im Navigationsbereich auf der linken Seite des Fensters. Wählen Sie im Kontextmenü dann entweder **Alle Bereiche in das Dienste-Skript exportieren** oder **Ausgewählte Bereiche in das Dienste-Skript exportieren**.

HINWEIS: Wenn Sie gerade zwei Logs miteinander vergleichen, ist kein Export in ein Dienste-Skript möglich.

5.6.4.2 Aufbau des Dienste-Skripts

In der ersten Zeile des Skriptheaders finden Sie Angaben zur Engine-Version (ev), zur Version der Benutzeroberfläche (gv) sowie zur Log-Version (lv). Über diese Angaben können Sie mögliche Änderungen an der XML-Datei verfolgen, über die das Skript erzeugt wird, und dadurch Inkonsistenzen bei der Ausführung vermeiden. An diesem Teil des Skripts sollten keine Änderungen vorgenommen werden.

Der Rest der Datei gliedert sich in mehrere Abschnitte, deren Einträge Sie bearbeiten können, um festzulegen, welche davon bei der Ausführung verarbeitet werden sollen. Um einen Eintrag für die Verarbeitung zu markieren, ersetzen Sie das davor stehende Zeichen „-“ durch ein „+“. Die einzelnen Skriptabschnitte sind jeweils durch eine Leerzeile voneinander getrennt. Jeder Abschnitt hat eine Nummer und eine Überschrift.

01) Running processes (Ausgeführte Prozesse)

Dieser Abschnitt enthält eine Liste mit allen Prozessen, die auf dem System ausgeführt werden. Für jeden Prozess ist der UNC-Pfad gefolgt vom CRC16-Hashwert in Sternchen (*) aufgeführt.

Beispiel:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In diesem Beispiel wurde der Prozess module32.exe ausgewählt, indem er mit dem Zeichen „+“ markiert wurde. Beim Ausführen des Skripts wird dieser Prozess beendet.

02) Loaded modules (Geladene Module)

Dieser Abschnitt enthält eine Liste der momentan verwendeten Systemmodule.

Beispiel:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In diesem Beispiel wurde das Modul khbekhb.dll mit einem „+“ markiert. Beim Ausführen des Skripts werden alle Prozesse, die dieses Modul verwenden, ermittelt und anschließend beendet.

03) TCP connections (TCP-Verbindungen)

Dieser Abschnitt enthält Informationen zu den aktiven TCP-Verbindungen.

Beispiel:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Beim Ausführen des Skripts wird der Eigentümer des Sockets der markierten TCP-Verbindungen ermittelt. Anschließend wird der Socket beendet, wodurch Systemressourcen wieder frei werden.

04) UDP endpoints (UDP-Endpunkte)

Dieser Abschnitt enthält Informationen zu den aktiven UDP-Endpunkten.

Beispiel:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Beim Ausführen des Skripts wird der Eigentümer des Sockets der markierten UDP-Verbindungen ermittelt. Anschließend wird der Socket beendet.

05) DNS server entries (DNS-Servereinträge)

Dieser Abschnitt enthält Angaben zur aktuellen DNS-Serverkonfiguration.

Beispiel:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Beim Ausführen des Skripts werden die markierten DNS-Servereinträge entfernt.

06) Important registry entries (Wichtige Registrierungseinträge)

Dieser Abschnitt enthält Informationen zu wichtigen Registrierungseinträgen.

Beispiel:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Beim Ausführen des Skripts werden die markierten Einträge gelöscht, auf eine Länge von 0 Byte abgeschnitten oder auf die Standardwerte zurückgesetzt. Was davon im Einzelfall geschieht, hängt von der Art des Eintrags und dem Wert des Schlüssels ab.

07) Services (Dienste)

Dieser Abschnitt enthält eine Liste der auf dem System registrierten Dienste.

Beispiel:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Beim Ausführen des Skripts werden die markierten Dienste samt davon abhängiger Dienste beendet und deinstalliert.

08) Drivers (Treiber)

Dieser Abschnitt enthält eine Liste der installierten Treiber.

Beispiel:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Beim Ausführen des Skripts werden die ausgewählten Treiber angehalten. Beachten Sie, dass einige Treiber nicht zulassen, angehalten zu werden.

09) Critical files (Kritische Dateien)

Dieser Abschnitt enthält Angaben zu Dateien, die für eine korrekte Funktion des Betriebssystems wesentlich sind.

Beispiel:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Die ausgewählten Objekte werden entweder gelöscht oder auf ihren ursprünglichen Wert zurückgesetzt.

5.6.4.3 Ausführen von Dienste-Skripten

Markieren Sie die gewünschten Elemente, speichern und schließen Sie das Skript. Führen Sie das fertige Skript dann direkt aus dem ESET SysInspector-Hauptfenster aus, indem Sie im Menü „Datei" auf **Dienste-Skript ausführen** klicken. Beim Öffnen eines Skripts wird die folgende Bestätigungsabfrage angezeigt: **Möchten Sie das Dienste-Skript „%Skriptname%" wirklich ausführen?** Nachdem Sie diese Abfrage bestätigt haben, erscheint unter Umständen eine weitere Warnmeldung, dass das auszuführende Dienste-Skript nicht signiert wurde. Klicken Sie auf **Starten**, um das Skript auszuführen.

Ein Dialogfenster mit der Bestätigung über die erfolgreiche Ausführung des Skripts wird angezeigt.

Wenn das Skript nur teilweise verarbeitet werden konnte, wird ein Dialogfenster mit der folgenden Meldung angezeigt: **Das Dienste-Skript wurde teilweise ausgeführt. Möchten Sie den Fehlerbericht anzeigen?** Wählen Sie **Ja**, um einen ausführlichen Fehlerbericht mit Informationen zu den nicht ausgeführten Aktionen anzuzeigen.

Wenn das Skript nicht erkannt wurde, wird ein Dialogfenster mit der folgenden Meldung angezeigt: **Das ausgewählte Dienste-Skript trägt keine Signatur. Wenn Sie unbekannte Skripte und Skripte ohne Signatur ausführen, können die Daten Ihres Computers beschädigt werden. Möchten Sie das Skript und die Aktionen wirklich ausführen?** Eine solche Meldung kann durch Inkonsistenzen im Skript verursacht werden (beschädigter Header, beschädigte Abschnittsüberschrift, fehlende Leerzeile zwischen Bereichen usw.). Sie können dann entweder die Skriptdatei öffnen und die Fehler beheben oder ein neues Dienste-Skript erstellen.

5.6.5 Häufig gestellte Fragen (FAQ)

Muss ESET SysInspector mit Administratorrechten ausgeführt werden?

ESET SysInspector muss zwar nicht unbedingt mit Administratorrechten ausgeführt werden, einige Informationen können jedoch nur über ein Administratorkonto erfasst werden. Führt ein Standardbenutzer oder ein Benutzer mit eingeschränkten Rechten das Programm aus, werden weniger Informationen über die Arbeitsumgebung zusammengestellt.

Erstellt ESET SysInspector eine Log-Datei?

ESET SysInspector kann eine Log-Datei mit der Konfiguration Ihres Computers erstellen. Um diese zu speichern, wählen Sie im Hauptprogrammfenster **Datei** > **Log speichern**. Logs werden im XML-Format gespeichert. Standardmäßig erfolgt dies im Verzeichnis *%USERPROFILE%\Eigene Dateien* und unter einem Namen nach dem Muster „SysInspector-%COMPUTERNAME%-JJMMTT-HHMM.XML". Falls Sie es vorziehen, können Sie Speicherort und -namen vor dem Speichern ändern.

Wie zeige ich eine ESET SysInspector-Log-Datei an?

Um eine von ESET SysInspector erstellte Log-Datei anzuzeigen, führen Sie das Programm aus und klicken Sie im Hauptprogrammfenster auf **Datei** > **Log öffnen**. Sie können Log-Dateien auch auf ESET SysInspector ziehen und dort ablegen. Wenn Sie häufig Log-Dateien aus ESET SysInspector anzeigen müssen, empfiehlt es sich, auf dem Desktop

eine Verknüpfung zur Datei SYSINSPECTOR.EXE anzulegen. So können Sie Log-Dateien einfach auf dieses Symbol ziehen, um sie zu öffnen. Aus Sicherheitsgründen ist es unter Windows Vista und Windows 7 ggf. nicht möglich, Dateien per Drag and Drop zwischen Fenstern mit unterschiedlichen Sicherheitsberechtigungen zu verschieben.

Ist eine Spezifikation für das Format der Log-Dateien verfügbar? Wie steht es um ein Software Development Kit (SDK)?

Zum gegenwärtigen Zeitpunkt sind weder eine Spezifikation noch ein SDK verfügbar, da sich das Programm noch in der Entwicklung befindet. Nach Veröffentlichung des Programms bieten wir diese möglicherweise an, abhängig von Kundenfeedback und Nachfrage.

Wie bewertet ESET SysInspector das Risiko, das von einem bestimmten Objekt ausgeht?

Um Objekten wie Dateien, Prozessen, Registrierungsschlüsseln usw. eine Risikostufe zuzuordnen, verwendet ESET SysInspector in der Regel einen Satz heuristischer Regeln, mit denen die Merkmale des Objekts untersucht werden, um anschließend nach entsprechender Gewichtung das Potenzial für schädliche Aktivitäten abzuschätzen. Basierend auf dieser Heuristik wird Objekten dann eine Risikostufe zugewiesen, von 1 - In Ordnung (grün) bis 9 - Risikoreich(rot). In der linken Navigationsanzeige sind Bereiche auf Grundlage der jeweils höchsten Risikostufe der Objekte in ihnen eingefärbt.

Bedeutet eine Risikostufe von „6 - Unbekannt (rot)“, dass ein Objekt gefährlich ist?

Die Einschätzung von ESET SysInspector legt nicht endgültig fest, ob eine Gefahr von einem Objekt ausgeht. Diese Entscheidung muss ein Sicherheitsexperte treffen. ESET SysInspector kann hierbei helfen, indem es dem Experten schnell zeigt, welche Objekte eventuell gründlicher untersucht werden müssen.

Warum stellt ESET SysInspector beim Start eine Verbindung ins Internet her?

Wie viele Anwendungen ist auch ESET SysInspector mit einem digitalen Zertifikat signiert, mit dem überprüft werden kann, dass die Software tatsächlich von ESET stammt und nicht verändert wurde. Um das Zertifikat zu verifizieren, kontaktiert das Betriebssystem eine Zertifizierungsstelle, welche die Identität des Softwareherstellers verifiziert. Dies ist ein normaler Vorgang für alle digital unterschriebenen Programme unter Microsoft Windows.

Was ist Anti-Stealth-Technologie?

Die Anti-Stealth-Technologie ermöglicht eine effektive Erkennung von Rootkits.

Wenn ein System von Schadcode angegriffen wird, das sich wie ein Rootkit verhält, ist der Benutzer möglicherweise dem Risiko von Schaden an seinen Daten oder deren Diebstahl ausgesetzt. Ohne ein spezielles Anti-Rootkit-Tool ist es beinahe unmöglich, ein Rootkit aufzuspüren.

Warum ist bei Dateien manchmal Microsoft als Unterzeichner angegeben, wenn gleichzeitig aber ein anderer Firmenname angezeigt wird?

Beim Versuch, die digitale Signatur einer ausführbaren Datei zu ermitteln, überprüft ESET SysInspector zuerst, ob in der Datei eine eingebettete Signatur vorhanden ist. Wenn eine digitale Signatur erkannt wird, wird die Datei mit den Informationen aus der Signatur validiert. Falls die zu überprüfende Datei keine digitale Signatur enthält, sucht ESI nach einer zugehörigen CAT-Datei (Sicherheitskatalog - *%systemroot%\system32\catroot*), die Informationen über die ausführbare Datei enthält. Falls eine entsprechende CAT-Datei existiert, wird deren digitale Signatur beim Überprüfungsprozess für die ausführbare Datei übernommen.

Aus diesem Grund sind einige Dateien mit „Signatur MS“ markiert, obwohl unter „Firmenname“ ein anderer Eintrag vorhanden ist.

Beispiel:

Windows 2000 enthält die Anwendung „HyperTerminal“ in *C:\Programme\Windows NT*. Die ausführbare Hauptdatei ist nicht digital signiert. In ESET SysInspector wird sie jedoch als von Microsoft signiert markiert. Dies liegt daran, dass in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* ein Verweis auf *C:\Programme\Windows NT\hypertrm.exe* (die Haupt-Programmdatei von HyperTerminal) vorhanden ist und *sp4.cat* wiederum durch Microsoft digital signiert wurde.

5.6.6 ESET SysInspector als Teil von ESET Smart Security

Um den ESET SysInspector-Bereich in ESET Smart Security zu öffnen, klicken Sie auf **Tools** > **ESET SysInspector**. Das Verwaltungssystem im ESET SysInspector-Fenster ähnelt dem von Prüfungslogs oder geplanten Tasks. Alle Vorgänge mit Systemsnapshots - Erstellen, Anzeigen, Vergleichen, Entfernen und Exportieren - sind mit einem oder zwei Klicks zugänglich.

Das ESET SysInspector-Fenster enthält Basisinformationen zum erstellten Snapshot wie z. B. Erstellungszeitpunkt, kurzer Kommentar, Name des Benutzers, der den Snapshot erstellt hat, sowie den Status des Snapshots.

Zum Vergleichen, Erstellen oder Löschen von Snapshots verwenden Sie die entsprechenden Schaltflächen unter der Snapshot-Liste im ESET SysInspector-Fenster. Diese Optionen sind ebenfalls im Kontextmenü verfügbar. Um den gewählten Systemsnapshot anzuzeigen, wählen Sie im Kontextmenü die Option **Anzeigen** aus. Um den gewünschten Snapshot in eine Datei zu exportieren, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Exportieren...**.

Die einzelnen Befehle sind nachstehend noch einmal ausführlicher beschrieben:

- **Vergleichen** - Hiermit können Sie zwei vorhandene Logs vergleichen. Diese Funktion eignet sich dafür, alle Unterschiede zwischen dem aktuellen und einem älteren Log zu ermitteln. Um sie zu nutzen, müssen Sie zwei Snapshots zum Vergleich auswählen.
- **Erstellen...** - Erstellen eines neuen Eintrags. Hierzu müssen Sie zunächst einen kurzen Kommentar zum Snapshot eingeben. Der Erstellungsfortschritt (des aktuell erstellten Snapshots) wird in der Spalte **Status** angezeigt. Fertige Snapshots haben den Status **Erstellt**.
- **Löschen/Alle löschen** - Entfernt Einträge aus der Liste.
- **Exportieren...** - Speichert den ausgewählten Eintrag als XML-Datei (wahlweise auch komprimiert als ZIP-Datei).

5.7 ESET SysRescue

ESET SysRescue ist ein Dienstprogramm zum Erstellen eines bootfähigen Datenträgers mit einer der ESET Security-Lösungen (ESET NOD32 Antivirus, ESET Smart Security oder auch eines der serverorientierten Produkte). Der große Vorteil von ESET SysRescue ist, dass ESET Security damit unabhängig vom Betriebssystem auf dem jeweiligen Rechner ausgeführt werden kann und direkten Zugriff auf die Festplatte sowie das gesamte Dateisystem hat. Auf diese Weise lassen sich auch Infektionen entfernen, bei denen dies normalerweise (bei laufendem Betriebssystem usw.) nicht möglich wäre.

5.7.1 Mindestanforderungen

ESET SysRescue verwendet das Microsoft Windows Preinstallation Environment (Windows PE) Version 2.x, das wiederum auf Windows Vista basiert.

Windows PE ist Teil des kostenlosen Windows Automated Installation Kit (Windows AIK) bzw. Windows Assessment and Deployment Kit (WADK). Vor dem Erstellen von ESET SysRescue muss daher Windows AIK bzw. WADK installiert werden (http://go.eset.eu/AIK, http://www.microsoft.com/en-us/download/details.aspx?id=30652). Die Auswahl zwischen diesen beiden Paketen erfolgt je nach Version des Betriebssystems. Da die 32-Bit-Version von Windows PE unterstützt wird, muss beim Erstellen von ESET SysRescue auf 64-Bit-Systemen ein 32-Bit-Installationspaket von ESET Security verwendet werden. ESET SysRescue unterstützt Windows AIK 1.1 und höher sowie WADK 1.0 und höher.

Wählen Sie bei der Installation von Windows ADK nur die Pakete Bereitstellungstools und Windows-Vorinstallationsumgebung (Windows PE) aus. Aufgrund der Größe dieser Pakete (über 3,0 GB) ist zum Herunterladen eine Hochgeschwindigkeits-Internetverbindung erforderlich.

ESET SysRescue ist in ESET Security ab der Version 4.0 verfügbar.

Windows ADK unterstützt:

- Windows 8
- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2

Hinweis: ESET SysRescue ist in älteren Versionen von ESET-Produkten möglicherweise nicht für Windows 8 verfügbar. In diesem Fall sollten Sie ein Produkt-Upgrade durchführen oder einen ESET SysRescue-Datenträger unter einer anderen Version von Microsoft Windows erstellen.

Windows AIK unterstützt:

- Windows 7
- Windows Vista
- Windows XP Service Pack 2 mit KB926044
- Windows XP Service Pack 3

5.7.2 So erstellen Sie eine Rettungs-CD

Klicken Sie auf **Start** > **Programme** > **ESET** > **ESET Smart Security** > **ESET SysRescue**, um den ESET SysRescue-Assistenten zu starten.

Zuerst prüft der Assistent, ob Windows AIK oder ADK und ein geeignetes Gerät für die Erstellung des Bootmediums verfügbar sind. Wenn das Windows AIK oder ADK auf Ihrem Computer nicht installiert (bzw. beschädigt oder nicht korrekt installiert) ist, bietet Ihnen der Assistent die Möglichkeit, es zu installieren oder den Pfad zu Ihrem Windows AIK- bzw. ADK-Ordner anzugeben. (http://go.eset.eu/AIK, http://www.microsoft.com/en-us/download/details.aspx?id=30652).

HINWEIS: Aufgrund der Größe des Windows AIK (über 1 GB) ist zum Herunterladen eine Hochgeschwindigkeits-Internetverbindung erforderlich.

Wählen Sie bei der Installation von Windows ADK nur die Pakete Bereitstellungstools und Windows-Vorinstallationsumgebung (Windows PE) aus. Aufgrund der Größe dieser Pakete (über 3,0 GB) ist zum Herunterladen eine Hochgeschwindigkeits-Internetverbindung erforderlich.

Im nächsten Schritt wählen Sie das Zielmedium für ESET SysRescue aus.

5.7.3 Zielauswahl

Neben CD/DVD/USB können Sie ESET SysRescue auch in einer ISO-Datei speichern. Später können Sie dann das ISO-Abbild auf CD/DVD brennen oder es anderweitig verwenden (z. B. in einer virtuellen Umgebung wie VMware oder VirtualBox).

Beachten Sie beim Zielmedium USB, dass auf manchen Computern nicht von USB gestartet werden kann. Manche BIOS-Versionen melden Probleme mit der Kommunikation zwischen BIOS und Bootmanager (z. B. bei Windows Vista). In diesen Fällen wird der Bootvorgang mit der folgenden Fehlermeldung abgebrochen:

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attemping to read the boot configuration data
```

Wenn diese Fehlermeldung angezeigt wird, wählen Sie als Zielmedium CD anstelle von USB.

5.7.4 Einstellungen

Vor dem Erstellen von ESET SysRescue zeigt der Installationsassistent Kompilierungsparameter an. Diese können Sie über die Schaltfläche **Ändern** bearbeiten. Folgende Optionen stehen zur Verfügung:

- Ordner
- ESET Antivirus
- Erweitert
- Internetprotokoll
- Bootfähiges USB-Gerät (wenn ein USB-Gerät als Ziel ausgewählt ist)
- Brennen (wenn das CD-/DVD-Laufwerk als Ziel ausgewählt ist)

Die Option **Erstellen** ist deaktiviert, wenn kein MSI-Installationspaket angegeben wurde oder falls kein ESET Security-Produkt auf dem Computer installiert ist. Um ein Installationspaket auszuwählen, klicken Sie auf **Ändern** und dann auf die Registerkarte **ESET Antivirus**. Beachten Sie außerdem, dass die Option **Erstellen** nur dann aktiv ist, wenn Sie einen Benutzernamen und ein Passwort eingeben (**Ändern** > **ESET Antivirus**).

5.7.4.1 Ordner

Temporärer Ordner ist das Arbeitsverzeichnis für die bei der Kompilierung eines ESET SysRescue-Mediums erforderlichen Dateien.

ISO-Ordner ist der Ordner, in dem die fertige ISO-Datei nach Abschluss der Kompilierung gespeichert wird.

In der Liste auf dieser Registerkarte werden alle lokalen und verbundenen Netzlaufwerke mit dem jeweils verfügbaren freien Speicherplatz angezeigt. Falls sich einige der Ordner auf einem Laufwerk befinden, das nicht über ausreichend freien Speicherplatz verfügt, so wird empfohlen, ein anderes Laufwerk mit mehr freiem Speicher auszuwählen. Anderenfalls bricht die Kompilierung möglicherweise vorzeitig ab.

Externe Anwendungen - Hiermit können Sie zusätzliche Programme festlegen, die nach dem Starten von einem ESET SysRescue-Medium ausgeführt oder installiert werden.

Externe Anwendungen einschließen - Mit dieser Option können Sie externe Programme zur ESET SysRescue-Kompilation hinzufügen.

Ausgewählter Ordner - Ordner, in dem sich die Programme befinden, die zur ESET SysRescue-CD hinzugefügt werden sollen

5.7.4.2 ESET Antivirus

Beim Erstellen der ESET SysRescue-CD können Sie zwischen zwei Quellen für die vom Compiler zu verwendenden ESET-Dateien wählen.

ESS/EAV-Ordner - Es werden die bereits vorhandenen Dateien aus dem Ordner verwendet, in dem das ESET Security-Produkt auf dem Computer installiert ist.

MSI-Datei - Es werden die im MSI-Installationspaket enthaltenen Dateien verwendet.

Danach können Sie den Speicherort der .nup-Dateien ändern. Normalerweise sollte die Standardoption **ESS/EAV-Ordner/MSI-Datei** ausgewählt sein. In Ausnahmefällen kann ein benutzerdefinierter **Update-Ordner** ausgewählt werden, z. B. um eine ältere oder neuere Version der Signaturdatenbank zu verwenden.

Sie können eine der beiden folgenden Quellen für Benutzername und Passwort verwenden:

ESS/EAV-Installation - Benutzername und Passwort werden der vorhandenen Installation des ESET Security-Produkts entnommen.

Von Benutzer - Es werden der Benutzername und das Passwort verwendet, die Sie in den dazugehörigen Feldern eingeben.

HINWEIS: ESET Security auf der ESET SysRescue-CD wird entweder über das Internet oder über das ESET Security-Produkt aktualisiert, das auf dem Computer installiert ist, auf dem die ESET SysRescue-CD ausgeführt wird.

5.7.4.3 Erweiterte Einstellungen

Auf der Registerkarte **Erweitert** können Sie die ESET SysRescue-CD für die Größe des Arbeitsspeichers auf Ihrem Computer optimieren. Wenn Sie **576 MB oder mehr** wählen, wird der Inhalt der CD in den Arbeitsspeicher (RAM) geschrieben. Bei der Einstellung **weniger als 576 MB** findet im Betrieb von WinPE hingegen laufend ein Zugriff auf die Rettungs-CD statt.

Im Bereich **Externe Treiber** können Sie Treiber für Ihre Hardware (z. B. Netzwerkadapter) hinzufügen. Da WinPE auf Windows Vista SP1 basiert, ist eine breite Hardwareunterstützung gegeben. In manchen Fällen kann es jedoch vorkommen, dass Hardware nicht erkannt wird. In diesem Fall müssen Sie den Treiber von Hand hinzufügen. Zum Hinzufügen eines Treibers in die ESET SysRescue-Kompilierung stehen zwei Methoden zur Verfügung: manuell (klicken Sie auf **Hinzufügen**) oder automatisch (klicken Sie auf **Autom. Suche**). Bei der manuellen Methode müssen Sie den Pfad zur passenden .inf-Datei auswählen (die dazugehörige *.sys-Datei muss ebenfalls in diesem Ordner liegen). Bei der automatischen Methode wird der Treiber automatisch im Betriebssystem des aktuellen Computers gesucht. Diese Methode sollten Sie nur verwenden, wenn Sie ESET SysRescue später auf einem Computer mit derselben Hardware (z. B. Netzwerkadapter) wie dem Computer nutzen, auf dem Sie die ESET SysRescue-CD erstellt haben. Bei der Erstellung der ESET SysRescue-CD wird der Treiber integriert, sodass Sie ihn später nicht mehr suchen müssen.

5.7.4.4 Internetprotokoll

In diesem Bereich können Sie grundlegende Netzwerkinformationen konfigurieren und vordefinierte Verbindungen nach dem Ausführen von ESET SysRescue einrichten.

Wählen Sie **Automatische private IP-Adresse**, um die IP-Adresse automatisch vom DHCP-Server (Dynamic Host Configuration Protocol) abzurufen.

Alternativ kann bei dieser Netzwerkverbindung auch eine manuell eingegebene IP-Adresse (statische IP-Adresse) verwendet werden. Wählen Sie **Benutzerdefiniert** zur Konfiguration der entsprechenden IP-Einstellungen. Wenn Sie diese Option aktivieren, müssen Sie eine **IP-Adresse** eingeben, bei LAN- und Breitband-Internetverbindungen zusätzlich eine **Subnetzmaske**. Geben Sie bei **Bevorzugter DNS-Server** und **Alternativer DNS-Server** die IP-Adressen des primären und sekundären DNS-Servers ein.

5.7.4.5 Bootfähiges USB-Gerät

Falls Sie ein USB-Gerät als Zielmedium ausgewählt haben, können Sie eines der verfügbaren USB-Medien auf der Registerkarte **Bootfähiges USB-Gerät** auswählen (falls mehrere USB-Geräte vorhanden sind).

Wählen Sie das entsprechende Ziel-**Gerät** aus, auf dem ESET SysRescue installiert werden soll.

Warnung: Das ausgewählte USB-Gerät wird beim Erstellen von ESET SysRescue formatiert. Alle vorher auf dem Gerät gespeicherten Daten gehen dabei verloren.

Wenn Sie die Option **Schnellformatierung** auswählen, werden alle Dateien von der Partition entfernt, das Laufwerk wird aber nicht auf beschädigte Sektoren geprüft. Verwenden Sie diese Option nur, wenn Ihr USB-Gerät schon einmal formatiert wurde und Sie sicher sind, dass es nicht beschädigt ist.

5.7.4.6 Brennen

Wenn CD/DVD als Zielmedium ausgewählt ist, können Sie zusätzliche Brennparameter auf der Registerkarte **Brennen** angeben.

ISO-Datei löschen - Aktivieren Sie diese Option, um die temporäre ISO-Datei nach dem Erstellen der ESET SysRescue-CD zu löschen.

Löschen aktiviert - Sie können zwischen schnellem Löschen und vollständigem Löschen auswählen.

Brennerlaufwerk - Wählen Sie das Laufwerk zum Brennen aus.

Warnung: Dies ist die Voreinstellung. Falls Sie eine wiederbeschreibbare CD/DVD verwenden, werden alle zuvor darauf gespeicherten Daten gelöscht.

Der Bereich „Medium“ enthält Informationen über das aktuell in Ihrem CD-/DVD-Laufwerk eingelegte Medium.

Schreibgeschwindigkeit - Wählen Sie die gewünschte Geschwindigkeit in der Liste aus. Berücksichtigen Sie dabei die Fähigkeiten Ihres Brenners und den Typ des CD-/DVD-Rohlings.

5.7.5 Die Arbeit mit ESET SysRescue

Damit die Rettungs-CD (bzw. -DVD/-USB) wie erwartet funktioniert, müssen Sie Ihren Computer vom ESET SysRescue-Bootmedium starten. Die Bootpriorität kann im BIOS geändert werden. Alternativ können Sie während des Computerstarts auch das Bootmenü aufrufen. Hierzu wird abhängig von Ihrer Motherboard-/BIOS-Variante üblicherweise eine der Tasten F9-F12 verwendet.

Nach dem Hochfahren über das Bootmedium wird ESET Security gestartet. Da ESET SysRescue nur in bestimmten Situationen verwendet wird, sind manche Schutzmodule und Programmfunktionen nicht erforderlich, die bei ESET Security normalerweise fester Bestandteil sind. Die Liste wird auf **Computer prüfen** , **Update** und einige Bereiche in **Einstellungen** und **Tools** begrenzt. Die Aktualisierung der Signaturdatenbank ist die wichtigste Funktion von ESET SysRescue. Wir empfehlen Ihnen, das Programm vor dem Start einer Prüfung des Computers zu aktualisieren.

5.7.5.1 Verwenden des ESET SysRescue-Mediums

Nehmen wir einmal an, dass Computer im Netzwerk mit einem Virus infiziert wurden, der ausführbare Dateien (.exe) manipuliert. ESET Security ist in der Lage, alle infizierten Dateien zu bereinigen, ausgenommen die Datei *explorer.exe*, die selbst im abgesicherten Modus nicht bereinigt werden kann. Dies liegt daran, dass *explorer.exe* als einer der grundlegenden Windows-Prozesse auch im abgesicherten Modus gestartet wird. ESET Security kann bei dieser Datei keine Aktion ausführen, sodass sie infiziert bleibt.

In einer solchen Situation können Sie ESET SysRescue verwenden, um das Problem zu lösen. ESET SysRescue benötigt keine Komponenten des Host-Betriebssystems. Deshalb kann es alle Dateien der Festplatte verarbeiten (bereinigen, löschen).

5.8 Kommandozeile

Das Virenschutz-Modul von ESET Smart Security kann über die Kommandozeile gestartet werden, entweder manuell (mit dem Befehl „ecls“) oder über eine Batch-Datei („.bat“). Syntax zum Starten der Prüfung aus der Kommandozeile:

```
ecls [OPTIONEN..] DATEIEN..
```

Folgende Parameter und Switches stehen zur Verfügung, um die manuelle Prüfung über die Kommandozeile auszuführen:

Methoden

/base-dir=ORDNER	Module laden aus ORDNER
/quar-dir=ORDNER	Quarantäne-ORDNER
/exclude=MASKE	Dateien, die mit der MASKE übereinstimmen, von Prüfungen ausschließen
/subdir	Unterordner prüfen (Standardeinstellung)
/no-subdir	Unterordner nicht prüfen
/max-subdir-level=STUFE	Maximale Suchtiefe von Unterordnern bei Prüfungen
/symlink	Symbolischen Links folgen (Standardeinstellung)
/no-symlink	Symbolischen Links nicht folgen
/ads	ADS prüfen (Standard)
/no-ads	ADS nicht prüfen
/log-file=DATEI	Ausgabe in DATEI protokollieren
/log-rewrite	Ausgabedatei überschreiben (Standardeinstellung: Anhängen)
/log-console	Ausgabe in Konsole protokollieren (Standard)
/no-log-console	Ausgabe nicht in Konsole protokollieren
/log-all	Saubere Dateien auch in Log aufnehmen
/no-log-all	Saubere Dateien nicht in Log aufnehmen (Standardeinstellung)
/aind	Aktivitätsanzeige anzeigen
/auto	Alle lokalen Laufwerke prüfen und automatisch säubern

Einstellungen für Prüfungen

/files	Dateien prüfen (Standardeinstellung)
/no-files	Dateien nicht prüfen
/memory	Speicher prüfen
/boots	Bootsektoren prüfen
/no-boots	Bootsektoren nicht prüfen (Standard)
/arch	Archive prüfen (Standardeinstellung)
/no-arch	Archive nicht prüfen
/max-obj-size=GRÖSSE	Nur Dateien prüfen, die kleiner als GRÖSSE Megabyte sind (Standard: 0 = unbegrenzt)
/max-arch-level=TIEFE	Maximale Verschachtelungstiefe von Archiven bei Prüfungen
/scan-timeout=LIMIT	Archive maximal LIMIT Sekunden prüfen
/max-arch-size=GRÖSSE	Nur Dateien in Archiven prüfen, die kleiner als GRÖSSE sind (Standard: 0 = unbegrenzt)
/max-sfx-size=GRÖSSE	Nur Dateien in selbstentpackenden Archiven prüfen, die kleiner als GRÖSSE Megabyte sind (Standard: 0 = unbegrenzt)
/mail	E-Mail-Dateien prüfen (Standard)
/no-mail	E-Mail-Dateien nicht prüfen
/mailbox	Postfächer prüfen (Standard)
/no-mailbox	Postfächer nicht prüfen
/sfx	Selbstentpackende Archive prüfen (Standard)
/no-sfx	Selbstentpackende Archive nicht prüfen
/rtp	Laufzeitkomprimierte Dateien prüfen (Standard)
/no-rtp	Laufzeitkomprimierte Dateien nicht prüfen
/adware	Adware/Spyware/Riskware erkennen (Standard)
/no-adware	Nicht auf Adware/Spyware/Riskware prüfen
/unsafe	Auf potenziell unsichere Anwendungen prüfen
/no-unsafe	Potenziell unsichere Anwendungen nicht prüfen (Standard)
/unwanted	Auf evtl. unerwünschte Anwendungen prüfen
/no-unwanted	Evtl. unerwünschte Anwendungen nicht prüfen (Standard)
/pattern	Signaturdatenbank verwenden (Standard)
/no-pattern	Signaturdatenbank nicht verwenden
/heur	Heuristik aktivieren (Standard)
/no-heur	Heuristik deaktivieren
/adv-heur	Advanced Heuristik aktivieren (Standard)
/no-adv-heur	Advanced Heuristik deaktivieren
/ext=ERWEITERUNGEN	Nur Dateien mit vorgegebenen ERWEITERUNGEN prüfen (Trennzeichen Doppelpunkt)
/ext-exclude=ERWEITERUNGEN	ERWEITERUNGEN (Trennzeichen Doppelpunkt) nicht prüfen
/clean-mode=MODUS	Säuberungs-MODUS für infizierte Objekte verwenden. Verfügbare Optionen: none (nicht säubern), standard (Standard), strict (strikt), rigorous (rigoros), delete (Löschen)
/quarantine	Infizierte Dateien in die Quarantäne kopieren (ergänzt die beim Säubern ausgeführte Aktion)
/no-quarantine	Infizierte Dateien nicht in die Quarantäne kopieren

Allgemeine Optionen

/help	Hilfe anzeigen und beenden
/version	Versionsinformationen anzeigen und beenden
/preserve-time	Datum für „Geändert am“ beibehalten

Exitcodes

0	Keine Bedrohungen gefunden
1	Bedrohungen gefunden und entfernt
10	Einige Dateien konnten nicht geprüft werden (evtl. Bedrohungen)
50	Bedrohung gefunden

100	Fehler

HINWEIS: Exitcodes größer 100 bedeuten, dass die Datei nicht geprüft wurde und daher infiziert sein kann.

6. Glossar

6.1 Schadsoftwaretypen

Bei Schadsoftware handelt es sich um bösartige Software, die versucht, in einen Computer einzudringen und/oder auf einem Computer Schaden anzurichten.

6.1.1 Viren

Ein Computervirus ist Schadcode, der an vorhandene Dateien auf Ihrem Computer vorangestellt oder angehängt wird. Ihren Namen haben sie nicht umsonst mit den Viren aus der Biologie gemein. Schließlich verwenden sie ähnliche Techniken, um sich von einem zum anderen Computer auszubreiten. Der Begriff „Virus“ wird jedoch häufig fälschlicherweise für eine beliebige Art von Bedrohung verwendet. Heute setzt sich mehr und mehr der neue, treffendere Ausdruck „Malware“ (Schadcode; engl. bösartige Software) durch.

Computerviren greifen hauptsächlich ausführbare Dateien und Dokumente an. Und so funktioniert ein Computervirus: Beim Ausführen einer infizierten Datei wird zunächst der Schadcode aufgerufen und ausgeführt, noch bevor die ursprüngliche Anwendung ausgeführt wird. Viren können beliebige Dateien infizieren, für die der aktuelle Benutzer über Schreibberechtigungen verfügt.

Computerviren unterscheiden sich nach Art und Schweregrad der durch sie verursachten Schäden. Einige von ihnen sind aufgrund ihrer Fähigkeit, Dateien von der Festplatte gezielt zu löschen, äußerst gefährlich. Andererseits gibt es aber auch Viren, die keinen Schaden verursachen. Ihr einziger Zweck besteht darin, den Benutzer zu verärgern und die technischen Fähigkeiten ihrer Urheber unter Beweis zu stellen.

Wenn Ihr Computer mit einem Virus infiziert ist und ein Säubern nicht möglich ist, senden Sie die Datei zur genaueren Prüfung an ESET. In einigen Fällen können infizierte Dateien so stark geändert werden, dass eine Säuberung nicht möglich ist und die Datei durch eine saubere Kopie ersetzt werden muss.

6.1.2 Würmer

Bei einem Computerwurm handelt es sich um ein Programm, das Schadcode enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Der grundlegende Unterschied zwischen Viren und Würmern besteht darin, dass Würmer in der Lage sind, sich selbstständig zu vermehren und zu verbreiten. Sie sind unabhängig von Hostdateien (oder Bootsektoren). Würmer verbreiten sich an die E-Mail-Adressen in Ihrer Kontaktliste oder nutzen Sicherheitslücken von Anwendungen in Netzwerken.

Daher sind Würmer wesentlich funktionsfähiger als Computerviren. Aufgrund der enormen Ausdehnung des Internets können sich Würmer innerhalb weniger Stunden und sogar Minuten über den gesamten Globus verbreiten. Da sich Würmer unabhängig und rasant vermehren können, sind sie gefährlicher als andere Arten von Schadsoftware.

Ein innerhalb eines Systems aktivierter Wurm kann eine Reihe von Unannehmlichkeiten verursachen: Er kann Dateien löschen, die Systemleistung beeinträchtigen oder Programme deaktivieren. Aufgrund ihrer Beschaffenheit können Würmer als Transportmedium für andere Arten von Schadcode fungieren.

Wurde Ihr Computer mit einem Wurm infiziert, empfiehlt es sich, alle betroffenen Dateien zu löschen, da sie höchstwahrscheinlich Schadcode enthalten.

6.1.3 Trojaner

Trojaner (trojanische Pferde) galten früher als eine Klasse von Schadprogrammen, die sich als nützliche Anwendungen tarnen, um den Benutzer zur Ausführung zu verleiten.

Da es sich hierbei um eine sehr breite Kategorie handelt, werden „Trojaner“ oft in mehrere Unterkategorien unterteilt:

- **Downloader** - Schadcode, der das Herunterladen anderer Bedrohungen aus dem Internet verursacht
- **Dropper** - Schadcode, der andere Arten von Schadcode auf gefährdete Computer verteilen kann
- **Backdoor** - Schadcode, der Remote-Angreifern die Möglichkeit gibt, auf den Computer zuzugreifen und ihn zu steuern
- **Keylogger** - Programm, das die Tastenanschläge eines Benutzers aufzeichnet und die Informationen an Angreifer sendet.
- **Dialer** - Schadcode, der Verbindungen zu teuren Einwahlnummern herstellt. Dass eine neue Verbindung erstellt wurde, ist für den Benutzer nahezu unmöglich festzustellen. Dialer sind nur eine Gefahr für Benutzer von Einwahlmodems. Diese werden allerdings nur noch selten eingesetzt.

Wenn auf Ihrem Computer eine Datei als Trojaner identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit ausschließlich Schadcode enthält.

6.1.4 Rootkits

Rootkits sind bösartige Programme, die Hackern unbegrenzten und verdeckten Zugriff auf ein System verschaffen. Nach dem Zugriff auf ein System (in der Regel unter Ausnutzung einer Sicherheitslücke) greifen Rootkits auf Funktionen des Betriebssystems zurück, um nicht von der Virenschutz-Software erkannt zu werden: Prozesse, Dateien und Windows-Registrierungsdaten werden versteckt. Aus diesem Grund ist es nahezu unmöglich, Rootkits mithilfe der üblichen Prüfmethoden zu erkennen.

Rootkits können auf zwei verschiedenen Ebenen entdeckt werden:

1. Beim Zugriff auf ein System. Die Rootkits haben das System noch nicht befallen, sind also inaktiv. Die meisten Virenschutzsysteme können Rootkits auf dieser Ebene entfernen (vorausgesetzt, dass solche Dateien auch als infizierte Dateien erkannt werden).
2. Wenn sie sich vor der üblichen Prüfung verbergen. Die Anti-Stealth-Technologie von ESET Smart Security kann auch aktive Rootkits erkennen und entfernen.

6.1.5 Adware

Adware ist eine Abkürzung für durch Werbung (engl. Advertising) unterstützte Software. In diese Kategorie fallen Programme, die zur Anzeige von Werbung dienen. Adware-Anwendungen öffnen häufig in Internetbrowsern neue Popup-Fenster mit Werbung oder ändern die Startseite des Browsers. Adware gehört oftmals zu Freeware-Programmen, damit deren Entwickler auf diesem Weg die Entwicklungskosten ihrer (gewöhnlich nützlichen) Anwendungen decken können.

Adware selbst ist nicht gefährlich - allerdings werden die Benutzer mit Werbung belästigt. Bedenklich ist Adware, insofern sie auch dazu dienen kann, Daten zu sammeln (wie es bei Spyware der Fall ist).

Wenn Sie sich dafür entscheiden, ein Freeware-Produkt zu verwenden, sollten Sie bei der Installation besonders aufmerksam sein. Die meisten Installationsprogramme benachrichtigen Sie über die Installation eines zusätzlichen Adware-Programms. In vielen Fällen ist es möglich, diesen Teil der Installation abzubrechen und das Programm ohne Adware zu installieren.

In einigen Fällen lassen sich Programme jedoch nicht ohne die Adware installieren, oder nur mit eingeschränktem Funktionsumfang. Das bedeutet, dass Adware häufig ganz „legal“ auf das System zugreift, da sich die Benutzer damit einverstanden erklärt haben. In diesem Fall gilt: Vorsicht ist besser als Nachsicht. Wird auf Ihrem Computer ein Adware-Programm entdeckt, sollten Sie die Datei löschen, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

6.1.6 Spyware

Der Begriff „Spyware“ fasst alle Anwendungen zusammen, die vertrauliche Informationen ohne das Einverständnis/ Wissen des Benutzers versenden. Diese Programme verwenden Überwachungsfunktionen, um verschiedene statistische Daten zu versenden, z. B. eine Liste der besuchten Websites, E-Mail-Adressen aus dem Adressbuch des Benutzers oder eine Auflistung von Tastatureingaben.

Die Entwickler von Spyware geben vor, auf diesem Weg die Interessen und Bedürfnisse der Benutzer erkunden zu wollen. Ziel sei es, gezieltere Werbeangebote zu entwickeln. Das Problem dabei ist, dass nicht wirklich zwischen nützlichen und bösartigen Anwendungen unterschieden werden kann. Niemand kann sicher sein, dass die gesammelten Informationen nicht missbraucht werden. Die von Spyware gesammelten Daten enthalten möglicherweise Sicherheitscodes, PINs, Kontonummern usw. Spyware wird oft im Paket mit der kostenlosen Version eines Programms angeboten, um so Einkünfte zu erzielen oder einen Anreiz für den Erwerb der kommerziellen Version zu schaffen. Oft werden die Benutzer bei der Programminstallation darüber informiert, dass Spyware eingesetzt wird, um sie damit zu einem Upgrade auf die kommerzielle, Spyware-freie Version zu bewegen.

Beispiele für bekannte Freeware-Produkte, die zusammen mit Spyware ausgeliefert werden, sind Client-Anwendungen für P2P-Netzwerke. Programme wie Spyfalcon oder Spy Sheriff gehören zur einer besonderen Kategorie von Spyware: Getarnt als Spyware-Schutzprogramme üben sie selbst Spyware-Funktionen aus.

Wenn auf Ihrem Computer eine Datei als Spyware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

6.1.7 Packprogramme

Ein Packprogramm ist eine selbstextrahierende, ausführbare Anwendung, mit der verschiedene Arten Malware in einem einzigen Paket gebündelt werden können.

Zu den bekanntesten Packprogrammen zählen UPX, PE_Compact, PKLite und ASPack. Die Erkennung einer bestimmten Malware unterscheidet sich je nach dem verwendeten Packprogramm. Packprogramme können außerdem ihre „Signatur“ verändern, sodass die Malware schwieriger zu erkennen und zu entfernen ist.

6.1.8 Potenziell unsichere Anwendungen

Es gibt zahlreiche seriöse Programme, die die Verwaltung miteinander vernetzter Computer vereinfachen sollen. Wenn sie aber in die falschen Hände geraten, kann mit ihnen Schaden angerichtet werden. Mit ESET Smart Security können solche Bedrohungen erkannt werden.

Zur Kategorie der **Potenziell unsicheren Anwendungen** zählen Programme, die zwar erwünscht sind, jedoch potenziell gefährliche Funktionen bereitstellen. Dazu zählen beispielsweise Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden).

Sollten Sie feststellen, dass auf Ihrem Computer eine potenziell unsichere Anwendung vorhanden ist (die Sie nicht selbst installiert haben), wenden Sie sich an Ihren Netzwerkadministrator oder entfernen Sie die Anwendung.

6.1.9 Evtl. unerwünschte Anwendungen

Eventuell unerwünschte Anwendungen sind Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, aber auf Leistung und Verhalten Ihres Computers negative Auswirkungen haben können. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Stand vor der Installation). Die gravierendsten Veränderungen sind:

- Neue Fenster werden angezeigt (Popup-Fenster, Werbung).
- Versteckte Prozesse werden ausgeführt.
- Prozessor und Speicher werden stärker belastet als zuvor.
- Suchergebnisse ändern sich.
- Die Anwendung kommuniziert mit Servern im Internet.

6.2 Angriffe

Es gibt zahlreiche spezielle Techniken, die es Angreifern ermöglichen, fremde Systeme zu beeinträchtigen. Dabei unterscheidet man mehrere Kategorien.

6.2.1 DoS-Angriffe

DoS- bzw. *Denial of Service*-Angriffe zielen darauf ab, Computer oder Netzwerke für die eigentlichen Nutzer unzugänglich zu machen. Die Kommunikation zwischen betroffenen Benutzern wird behindert und geht nicht mehr ordnungsgemäß vonstatten. In der Regel müssen Sie einen Computer, der einem DoS-Angriff ausgesetzt ist, neu starten. Nur so ist der ordnungsgemäße Betrieb wiederherzustellen.

In den meisten Fällen sind Webserver betroffen. Ziel solcher Angriffe ist es, die Verfügbarkeit der Webserver für einen bestimmten Zeitraum auszusetzen.

6.2.2 DNS Poisoning

Mit der Technik „DNS (Domain Name Server) Poisoning" können Hacker DNS-Server beliebiger Computer über die Echtheit eingeschleuster Daten täuschen. Die falschen Informationen werden für eine bestimmte Zeit im Cache gespeichert. Angreifer können dann DNS-Antworten von IP-Adressen umschreiben. Dies hat zur Folge, dass Benutzer beim Zugriff auf eine Internet-Website nicht den Inhalt der Website, sondern Computerviren oder Würmer herunterladen.

6.2.3 Angriffe von Würmern

Bei einem Computerwurm handelt es sich um ein Programm, das bösartigen Code enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Netzwerkwürmer machen sich Sicherheitslücken verschiedener Anwendungen zu Nutze. Aufgrund der Verfügbarkeit des Internets können sie sich innerhalb weniger Stunden nach ihrer Freigabe über den gesamten Globus verbreiten.

Ein Großteil der Wurmangriffe (Sasser, SqlSlammer) lässt sich durch Anwendung der Standardsicherheitseinstellungen der Firewall oder durch das Blockieren ungeschützter und unbenutzter Ports vermeiden. Darüber hinaus ist es unerlässlich, dass Sie auf Ihrem System regelmäßig Updates mit den neuesten Sicherheitspatches durchführen.

6.2.4 Portscans (Port Scanning)

Beim Port Scanning wird ein Netzwerkhost auf offene Computerports untersucht. Ein Portscanner ist eine Software zur Erkennung solcher Ports.

Bei einem Computerport handelt es sich um einen virtuellen Punkt zur Abwicklung von ein- und ausgehenden Daten. Für die Sicherheit spielen Ports eine zentrale Rolle. In einem großen Netzwerk können die von Portscannern gesammelten Informationen dazu beitragen, mögliche Sicherheitslücken ausfindig zu machen. Diese Art der Nutzung ist legitim.

Dennoch wird Port Scanning oft von Hackern missbraucht, um Sicherheitsbestimmungen zu unterlaufen. In einem ersten Schritt werden Pakete an jeden Port gesendet. Aus der Art der Rückmeldung lässt sich ableiten, welche Ports verwendet werden. Der Port Scanning-Vorgang selbst verursacht keinen Schaden. Seien Sie sich jedoch im Klaren darüber, dass auf diese Weise Sicherheitslücken aufgedeckt werden können und Angreifer dadurch die Möglichkeit haben, die Kontrolle über Remotecomputer zu übernehmen.

Netzwerkadministratoren wird geraten, alle inaktiven Ports zu blockieren und alle aktiven Ports vor einem unerlaubten Zugriff zu schützen.

6.2.5 TCP Desynchronization

Die Technik der TCP Desynchronization wird für TCP-Hijacking-Angriffe eingesetzt. Die TCP Desynchronization wird ausgelöst, wenn die Laufnummer der eingehenden Pakete sich von der erwarteten Laufnummer unterscheidet. Pakete mit unerwarteter Laufnummer werden verworfen (oder im Pufferspeicher gespeichert, wenn sie im aktuellen Kommunikationsfenster vorkommen).

Bei der Desynchronization verwerfen beide Kommunikationsendpunkte empfangene Pakete. Das ist der Zeitpunkt, an dem Angreifer Schadcode und Pakete mit der richtigen Laufnummer einschleusen können. Die Angreifer können die Kommunikation auch manipulieren und anpassen.

TCP-Hijacking-Angriffe zielen auf die Unterbrechung von Server-Client- bzw. P2P-Verbindungen. Viele Angriffe können durch Authentifizierungsmaßnahmen für jedes TCP-Segment vermieden werden. Sie sollten Ihre Netzwerkgeräte außerdem gemäß Empfehlung konfigurieren.

6.2.6 SMB Relay

SMBRelay und SMBRelay2 sind besondere Programme zum Ausführen von Angriffen auf Remotecomputer. Die Programme nutzen das SMB-Protokoll für den gemeinsamen Datenzugriff, das auf NetBIOS aufbaut. Die Freigabe eines Ordners oder eines Verzeichnisses im LAN erfolgt in der Regel mittels des SMB-Protokolls.

Im Rahmen der lokalen Netzwerkkommunikation werden Passwort-Hash-Werte ausgetauscht.

SMBRelay empfängt eine Verbindung über die UDP-Ports 139 und 445, leitet die zwischen Client und Server ausgetauschten Pakete weiter und manipuliert sie. Nachdem die Verbindung hergestellt wurde und die Authentifizierung erfolgt ist, wird die Verbindung zum Client getrennt. SMBRelay erstellt eine neue virtuelle IP-Adresse. Auf die neue Adresse kann über den Befehl „net use \\192.168.1.1“ zugegriffen werden. Jede der Windows-Netzwerkfunktionen kann dann auf diese Adresse zugreifen. Bis auf Aushandlungs- und Authentifizierungdaten leitet SMBRelay alle SMB-Protokoll-Daten weiter. Angreifer können die IP-Adresse verwenden, solange der Client-Computer verbunden ist.

SMBRelay2 funktioniert nach demselben Prinzip wie SMBRelay, verwendet aber NetBIOS-Namen statt IP-Adressen. Beide können Man-in-the-Middle-Angriffe ausführen. Über diese Art von Angriffen können Angreifer Nachrichten, die zwischen zwei Kommunikationsendpunkten ausgetauscht werden, unbemerkt lesen und manipulieren. Computer, die solchen Angriffen ausgesetzt sind, senden häufig keine Antwort mehr oder führen ohne ersichtlichen Grund einen Neustart aus.

Um Angriffe zu vermeiden, sollten Sie Authentifizierungspasswörter oder -schlüssel verwenden.

6.2.7 ICMP-Angriffe

ICMP (Internet Control Message Protocol) ist ein weit verbreitetes Internetprotokoll. Es wird vor allem verwendet, um Fehlermeldungen von vernetzten Computern zu senden.

Angreifer versuchen, die Schwachstellen des ICMP-Protokolls auszunutzen. Das ICMP-Protokoll wird für einseitige Kommunikation eingesetzt, bei der keine Authentifizierung erforderlich ist. Dadurch können Angreifer sogenannte DoS (Denial of Service)-Angriffe starten oder Angriffe ausführen, durch die nicht autorisierte Personen auf eingehende und ausgehende Datenpakete zugreifen können.

Typische Beispiele für ICMP-Angriffe sind Ping-Flood, ICMP_ECHO-Flood und Smurf-Attacken. Bei einem ICMP-Angriff arbeitet der Computer deutlich langsamer (dies gilt für alle Internetanwendungen), und es treten Probleme mit der Internetverbindung auf.

6.3 ESET-Technologie

6.3.1 Exploit-Blocker

Der Exploit-Blocker sichert besonders anfällige Anwendungstypen wie Webbrowser, PDF-Leseprogramme, E-Mail-Programme und MS Office-Komponenten ab. Er überwacht das Verhalten von Prozessen auf verdächtige Aktivitäten, die auf einen Exploit hinweisen könnten.

Wenn der Exploit-Blocker einen verdächtigen Prozess identifiziert, kann er ihn sofort anhalten und Daten über die Bedrohung erfassen, die dann an das ESET Live Grid-Cloudsystem gesendet werden. Diese Daten werden durch ESET analysiert und genutzt, um alle Anwender besser vor unbekannten Bedrohungen und neuesten Angriffen durch Malware, für die noch keine Erkennungssignaturen vorhanden sind, zu schützen.

6.3.2 Erweiterte Speicherprüfung

Die erweiterte Speicherprüfung bietet im Zusammenspiel mit dem Exploit-Blocker stärkeren Schutz vor Malware, die darauf ausgelegt ist, der Erkennung durch Anti-Malware-Produkte mittels Verschleierung und/oder Verschlüsselung zu entgehen. In Fällen, in denen herkömmliche Emulation oder Heuristik eine Bedrohung eventuell nicht aufspüren, kann die erweiterte Speicherprüfung verdächtiges Verhalten identifizieren und Bedrohungen erkennen, wenn sie sich im Arbeitsspeicher manifestieren. Diese Lösung kann selbst gegen stark verschleierte Malware wirkungsvoll agieren.

Anders als der Exploit-Blocker sucht die erweiterte Speicherprüfung nach ausgeführter Malware. Damit ist das Risiko verbunden, dass vor der Erkennung einer Bedrohung bereits schädliche Aktivitäten durchgeführt wurden; falls jedoch andere Erkennungsmethoden versagt haben, bietet sie eine zusätzliche Schutzebene.

6.3.3 Schwachstellen-Schutz

Der Schwachstellen-Schutz ist eine Erweiterung der Personal Firewall, die die Erkennung bekannter Schwachstellen auf Netzwerkebene verbessert. Durch Bereitstellung von Erkennungsmethoden für verbreitete Schwachstellen in häufig genutzten Protokollen wie SMB, RPC und RDP bietet er eine weitere wichtige Schutzebene gegen die Verbreitung von Malware, Angriffe aus dem Netzwerk und das Ausnützen von Sicherheitslücken, für die noch kein Patch herausgegeben oder installiert wurde.

6.3.4 ESET Live Grid

ESET Live Grid basiert auf dem ThreatSense.Net®-Frühwarnsystem; es arbeitet mit Daten, die ESET-Anwender weltweit übermitteln, und sendet sie an das ESET-Virenlabor. ESET Live Grid stellt verdächtige Proben und Metadaten „aus freier Wildbahn“ bereit und gibt uns so die Möglichkeit, unmittelbar auf die Anforderungen unserer Kunden zu reagieren und sie vor den neuesten Bedrohungen zu schützen. Die ESET-Malwareforscher gewinnen aus diesen Informationen ein präzises Bild von Eigenschaften und Umfang aktueller weltweiter Bedrohungen, wodurch wir uns auf die relevanten Ziele konzentrieren können. ESET Live Grid-Daten spielen eine wichtige Rolle, Prioritäten in unserer automatisierten Datenverarbeitung zu setzen.

Zudem wird ein Reputations-Check umgesetzt, der die Effizienz unserer Anti-Malware-Lösung insgesamt weiter steigern kann. Wenn eine ausführbare Datei oder ein Archiv im System eines Anwenders untersucht werden, wird als erstes das Hash-Tag mit einer Datenbank mit Positiv- und Negativeinträgen abgeglichen. Wird es auf der Positivliste gefunden, gilt die untersuchte Datei als sauber und wird bei zukünftigen Prüfungen übersprungen. Wenn es sich auf der Negativliste befindet, werden ja nach Art der Bedrohung geeignete Maßnahmen getroffen. Sollte keine Übereinstimmung gefunden werden, wird die Datei gründlich analysiert. Auf dieser Grundlage werden Dateien als Bedrohung oder keine Bedrohung kategorisiert. Dieser Ansatz wirkt sich sehr positiv auf die Prüfleistung aus.

Dieser Reputations-Check ermöglicht die effektive Erkennung von Malwareproben, selbst wenn ihre Signaturen noch nicht per Aktualisierung der Virusdatenbank auf den Computer des Anwenders übertragen wurden (was mehrmals täglich geschieht).

6.4 E-Mail

Die E-Mail („elektronische Post“) ist ein modernes Kommunikationsmittel mit vielen Vorteilen. Dank ihrer Flexibilität, Schnelligkeit und Direktheit spielte die E-Mail bei der Verbreitung des Internets in den frühen 1990er Jahren eine entscheidende Rolle.

Doch aufgrund der Anonymität, die E-Mails und das Internet bieten, wird diese Kommunikationsform auch häufig für illegale Aktivitäten wie das Versenden von Spam-Mails genutzt. Als „Spam“ gelten z. B. unerwünschte Werbeangebote, Hoaxes (Falschmeldungen) und E-Mails, mit denen Schadsoftware verbreitet werden soll. Die Belästigung und Gefährdung durch Spam wird zusätzlich dadurch gefördert, dass E-Mails praktisch kostenlos versendet werden können und den Verfassern von Spam-Mails verschiedenste Tools und Quellen zur Verfügung stehen, um an neue E-Mail-Adressen zu gelangen Die große Anzahl und Vielfalt, in der Spam-Mails auftreten, erschwert die Kontrolle. Je länger Sie eine E-Mail-Adresse verwenden, desto wahrscheinlicher ist es, dass diese in einer Spam-Datenbank erfasst wird. Einige Tipps zur Vorbeugung:

- Veröffentlichen Sie Ihre E-Mail-Adresse, soweit möglich, nicht im Internet
- Geben Sie Ihre E-Mail-Adresse nur an vertrauenswürdige Personen weiter
- Benutzen Sie, wenn möglich, keine üblichen Aliasnamen - bei komplizierten Aliasnamen ist die Wahrscheinlichkeit der Verfolgung niedriger
- Antworten Sie nicht auf Spam-Mails, die sich in Ihrem Posteingang befinden
- Seien Sie vorsichtig, wenn Sie Internetformulare ausfüllen - achten Sie insbesondere auf Optionen wie „Ja, ich möchte per E-Mail informiert werden“.
- Verwenden Sie separate E-Mail-Adressen - z. B. eine für Ihre Arbeit, eine für die Kommunikation mit Freunden usw.
- Ändern Sie Ihre E-Mail-Adresse von Zeit zu Zeit
- Verwenden Sie eine Spamschutz-Lösung

6.4.1 Werbung

Werbung im Internet ist eine der am schnellsten wachsenden Formen von Werbung. Die wesentlichen Vorteile für das Marketing liegen im geringen finanziellen Aufwand und dem hohen Grad von Direktheit. Davon abgesehen erreichen E-Mails die Empfänger fast ohne Zeitverzögerung. In vielen Unternehmen werden E-Mail-Marketingtools für eine effektive Kommunikation mit aktuellen und zukünftigen Kunden verwendet.

Da Sie Interesse an kommerziellen Informationen zu bestimmten Produkten haben könnten, handelt es sich dabei um rechtmäßige Werbung. Doch vielfach werden unerwünschte Massen-E-Mails mit Werbung versendet. In solchen Fällen ist die Grenze der E-Mail-Werbung überschritten, und diese E-Mails gelten als Spam.

Die Masse der unerwünschten E-Mails hat sich zu einem Problem entwickelt, ohne dass ein Nachlassen abzusehen ist. Die Verfasser unerwünschter E-Mails versuchen häufig, Spam-E-Mails wie rechtmäßige Nachrichten aussehen zu lassen.

6.4.2 Falschmeldungen (Hoaxes)

Ein Hoax ist eine Spam-Nachricht, die über das Internet verbreitet wird. Hoaxes werden im Allgemeinen per E-Mail oder über Kommunikationstools wie ICQ oder Skype versendet. Der Inhalt der Nachricht ist meist ein Scherz oder eine Falschmeldung.

Oft werden dabei Falschmeldungen zu angeblichen Computerviren verbreitet. Der Empfänger soll verunsichert werden, indem ihm mitgeteilt wird, dass sich auf seinem Computer ein „nicht identifizierbarer Virus“ befindet, der Dateien zerstört, Passwörter abruft oder andere schädliche Vorgänge verursacht.

Es kommt vor, dass ein Hoax den Empfänger auffordert, die Nachricht an seine Kontakte weiterzuleiten, wodurch er sich verbreitet. Es gibt verschiedenste Arten von Hoaxes - Mobiltelefon-Hoaxes, Hilferufe, Angebote zu Geldüberweisungen aus dem Ausland usw. Häufig ist es nicht möglich, die tatsächliche Absicht des Autors zu durchschauen.

Wenn Sie eine Nachricht lesen, in der Sie aufgefordert werden, diese an alle Ihre Kontakte weiterzuleiten, so handelt es sich möglicherweise um einen Hoax. Es gibt viele Internetseiten, auf denen Sie prüfen können, ob eine

E-Mail rechtmäßig ist oder nicht. Bevor Sie eine fragliche Nachricht weiterleiten, versuchen Sie über eine Internetsuche abzuklären, ob es sich um einen Hoax handelt.

6.4.3 Phishing

Der Begriff „Phishing“ bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Das Ziel von Phishing ist es, an vertrauliche Daten wie Kontonummern, PIN-Codes usw. heranzukommen.

Der Zugriff auf vertrauliche Informationen wird oft durch das Versenden von E-Mails erreicht, die von einer scheinbar vertrauenswürdigen Person bzw. von einem scheinbar seriösen Unternehmen (z. B. Finanzinstitution, Versicherungsunternehm) stammen. Eine solche E-Mail kann sehr echt aussehen. Grafiken und Inhalte wurden möglicherweise sogar von der Quelle entwendet, die nachgeahmt werden soll. Sie werden unter einem Vorwand (Datenprüfung, finanzielle Transaktionen usw.) aufgefordert, persönliche Daten einzugeben, wie Ihre Bankverbindung, Benutzernamen und Passwörter. Alle diese Daten, werden Sie denn übermittelt, können mühelos gestohlen oder missbraucht werden.

Banken, Versicherungen und andere rechtmäßige Unternehmen fragen nie in einer E-Mail nach Benutzername und Passwort.

6.4.4 Erkennen von Spam-Mails

Es gibt verschiedene Anzeichen, die darauf hindeuten, dass es sich bei einer bestimmten E-Mail in Ihrem Postfach um Spam handelt. Wenn eines oder mehrere der folgenden Kriterien zutreffen, handelt es sich höchstwahrscheinlich um eine Spam-Nachricht:

- Die Adresse des Absenders steht nicht in Ihrer Kontaktliste.
- Ihnen wird ein größerer Geldbetrag in Aussicht gestellt, Sie sollen jedoch zunächst eine kleinere Summe zahlen.
- Sie werden unter einem Vorwand (Datenprüfung, finanzielle Transaktionen usw.) aufgefordert, persönliche Daten einzugeben, wie Ihre Bankverbindung, Benutzernamen und Passwörter
- Die Nachricht ist in einer anderen Sprache verfasst.
- Sie werden aufgefordert, ein Produkt zu erwerben, das Sie nicht bestellt haben. Falls Sie das Produkt dennoch kaufen möchten, prüfen Sie, ob der Absender ein vertrauenswürdiger Anbieter ist (fragen Sie beim Hersteller nach).
- Einige Wörter sind falsch geschrieben, um den Spamfilter zu umgehen, z. B. „Vaigra“ statt „Viagra“ usw.

6.4.4.1 Regeln

Im Kontext von Spam-Schutz-Lösungen und E-Mail-Programmen dienen Regeln der Steuerung von E-Mail-Funktionen. Regeln setzen sich aus zwei logischen Teilen zusammen:

1. einer Bedingung (z. B. einer eingehenden Nachricht von einer bestimmten Adresse)
2. einer Aktion (z. B. das Löschen der Nachricht bzw. das Verschieben der Nachricht in einen angegebenen Ordner).

Je nach Virenschutzlösung gibt es unterschiedlich viele Regeln und Kombinationsmöglichkeiten. Die Regeln dienen als Maßnahme gegen Spam (unerwünschte E-Mail-Nachrichten). Typische Beispiele sind:

- 1. Bedingung: Eine eingehende E-Mail-Nachricht enthält einige der Wörter, die häufig in Spam-Nachrichten vorkommen
  2. Aktion: Nachricht löschen

- 1. Bedingung: Eine eingehende E-Mail-Nachricht enthält einen Anhang mit der Erweiterung EXE
  2. Aktion: Anhang löschen und Nachricht dem Postfach zustellen

- 1. Bedingung: Der Absender einer eingehenden Nachricht ist Ihr Arbeitgeber
  2. Aktion: Nachricht in den Ordner „Arbeit“ verschieben

Wir empfehlen Ihnen, in Spam-Schutz-Programmen verschiedene Regeln miteinander zu kombinieren, um die Verwaltung zu vereinfachen und den Spam-Schutz noch effektiver zu gestalten.

6.4.4.2 Positivliste

Im Allgemeinen handelt es sich bei einer Positivliste (auch „Whitelist“) um eine Liste von Objekten oder Personen, die akzeptiert werden oder denen eine Berechtigung eingeräumt worden ist. Der Begriff „E-Mail-Positivliste“ bezeichnet eine Liste von Kontakten, von denen der Nutzer Nachrichten erhalten möchte. Solche Positivlisten beruhen auf Stichwörtern, nach denen E-Mail-Adressen, Domain-Namen oder IP-Adressen durchsucht werden.

Ist bei einer Positivliste der „Exklusiv-Modus“ aktiviert, werden Nachrichten von jeder anderen Adresse, Domain oder IP-Adresse zurückgewiesen. Ist dieser Modus jedoch nicht aktiviert, werden solche Nachrichten nicht etwa gelöscht, sondern auf andere Art und Weise geprüft.

Eine Positivliste beruht somit auf dem entgegengesetzten Prinzip einer Negativliste („Blacklist“). Im Vergleich zu Negativlisten sind Positivlisten relativ pflegeleicht. Es wird empfohlen, sowohl eine Positiv- als auch eine Negativliste zu verwenden, damit Spam effektiver gefiltert werden kann.

6.4.4.3 Negativliste

Eine Negativliste oder „Blacklist“ bezeichnet im Allgemeinen eine Liste unerwünschter oder verbotener Personen oder Dinge. In der virtuellen Welt handelt es sich um eine Technik, die das Annehmen von E-Mail-Nachrichten aller Absender erlaubt, die nicht in einer solchen Liste stehen.

Es gibt zwei Arten von Negativlisten: solche, die vom Benutzer in seinem Spam-Schutz-Programm eingerichtet wurden, und professionelle, von spezialisierten Institutionen erstellte und regelmäßig aktualisierte Negativlisten, die im Internet verfügbar sind.

Das Verwenden von Negativlisten ist eine wesentliche Technik zur erfolgreichen Spam-Filterung, allerdings sind Negativlisten schwierig zu pflegen, da täglich neue Einträge anfallen. Für effektiven Spam-Schutz empfehlen wir Ihnen, sowohl eine Positivliste als auch eine Negativliste zu führen.

6.4.4.4 Serverseitige Kontrolle

Die serverseitige Kontrolle ist eine Technik zur Erkennung von massenweise versendeten Spam-E-Mails auf Basis der Anzahl empfangener Nachrichten und der Reaktionen von Benutzern. Jede E-Mail-Nachricht hinterlässt einen eindeutigen digitalen Footprint („Fußabdruck“), der sich nach dem Inhalt der Nachricht richtet. Diese eindeutige ID-Nummer lässt keine Rückschlüsse über den Inhalt zu. Zwei identische Nachrichten besitzen denselben Footprint, verschiedene E-Mails auch verschiedene Footprints.

Wenn eine E-Mail als Spam eingestuft wird, wird der Footprint dieser E-Mail an den Server gesendet. Wenn der Server weitere identische Footprints empfängt (die einer bestimmten Spam-E-Mail entsprechen), wird dieser Footprint in einer Datenbank gespeichert. Beim Prüfen eingehender E-Mails sendet das Programm die Footprints der E-Mails an den Server. Der Server gibt Informationen darüber zurück, welche Footprints E-Mails entsprechen, die von Benutzern bereits als Spam eingestuft worden sind.